Actualizar VMware ESXi

Actualización 3
VMware vSphere 8.0
VMware ESXi 8.0



Puede encontrar la documentación técnica más actualizada en el sitio web de VMware by Broadcom en:

https://docs.vmware.com/es/

VMware by Broadcom
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contenido

Acerca de Actualizar VMware ESXi

1

En el documento *Actualizar VMware ESXi*, se describe cómo actualizar VMware ESXi™ a la versión actual.

En VMware, valoramos la inclusión. Para fomentar este principio en nuestros clientes y clientas, partners y comunidad interna, hemos actualizado esta guía para eliminar las instancias de lenguaje no inclusivo.

Audiencia prevista

El documento *Actualizar VMware ESXi* está dirigido a quienes necesitan realizar una actualización a partir de versiones anteriores de ESXi. Estos temas están destinados a administradores de sistemas Microsoft Windows o Linux experimentados que estén familiarizados con las operaciones de los centros de datos y la tecnología de máquinas virtuales.

Opciones de actualización de vCenter Server

2

vCenter Server 8.0 ofrece muchas opciones para actualizar la implementación de vCenter Server. Para que la actualización de vCenter Server se realice correctamente, debe comprender las opciones de actualización, los detalles de configuración que influyen en el proceso de actualización y la secuencia de tareas.

Los dos componentes principales de vSphere son VMware ESXi™ y VMware vCenter Server™. ESXi es la plataforma de virtualización en la que se crean y se ejecutan las máquinas virtuales y los dispositivos virtuales. vCenter Server es un servicio que actúa como administrador central de los hosts ESXi conectados en una red. El sistema vCenter Server se utiliza para agrupar y administrar los recursos de varios hosts. vCenter Server Appliance es una máquina virtual preconfigurada y optimizada para ejecutar vCenter Server.

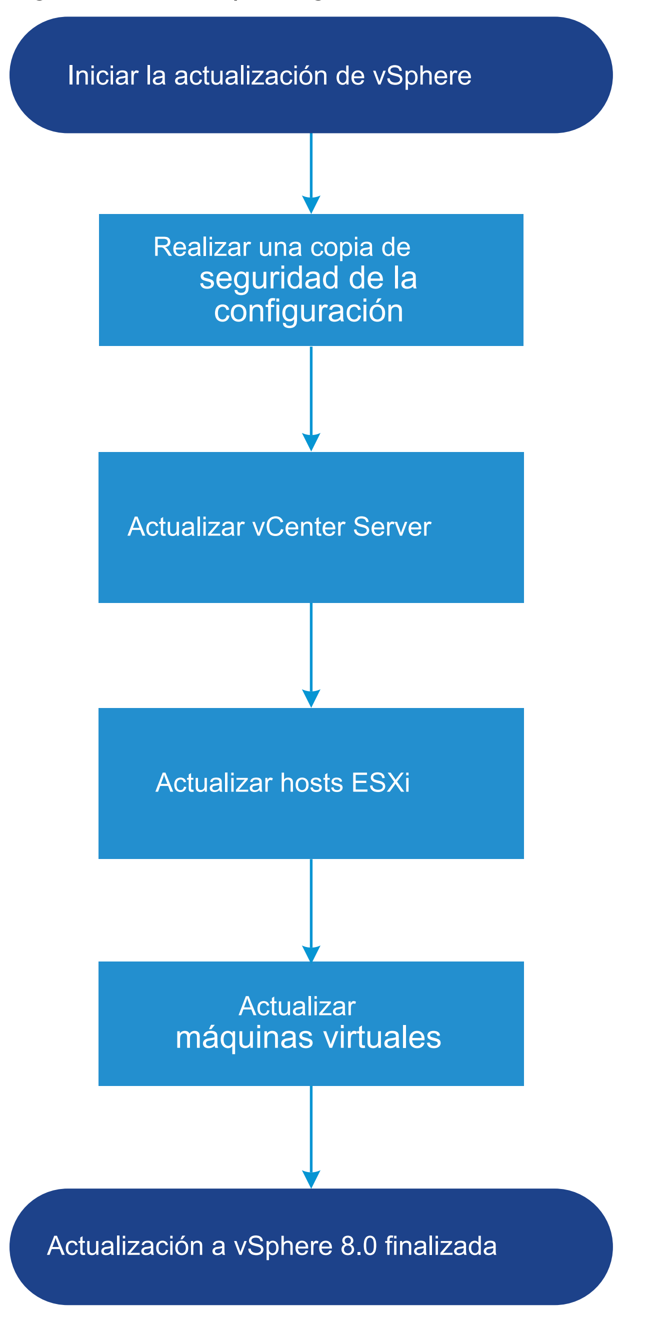
Puede actualizar las implementaciones existentes de vCenter Server que incluyan una instancia de Platform Services Controller integrada o externa a una implementación compuesta por una instancia de vCenter Server Appliance.

Lea los siguientes temas a continuación:

Descripción del proceso de actualización de vSphere

vSphere es un producto sofisticado con varios componentes para actualizar. Comprender la secuencia de tareas requeridas es esencial para actualizar correctamente vSphere.

Figura 2-1. Descripción general de las tareas de actualización de vSphere



La actualización de vSphere abarca las siguientes tareas:

1 Lea las notas de la versión de vSphere.

2 Compruebe que haya realizado una copia de seguridad de la configuración.

3 Si su sistema vSphere incluye soluciones o complementos de VMware, asegúrese de que sean compatibles con la versión de vCenter Server Appliance a la que va a actualizar. Consulte la *Matriz de interoperabilidad de productos VMware* en http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

4 Actualice vCenter Server.

Para obtener instrucciones detalladas, consulte Actualización de vCenter Server.

5 Actualice los hosts ESXi. Consulte Descripción general del proceso de actualización del host ESXi.

6 A fin de garantizar que el almacenamiento en disco para los archivos de registro sea suficiente, se recomienda instalar un servidor syslog para el registro remoto. La configuración del registro en un host remoto es especialmente importante para hosts con una cantidad limitada de almacenamiento local.

   Consulte Espacio libre necesario para registro del sistema y Configurar Syslog en hosts ESXi.

7 Actualice las máquinas virtuales de forma manual o mediante vSphere Lifecycle Manager para realizar una actualización organizada.

   Consulte Actualizar máquinas virtuales y VMware Tools

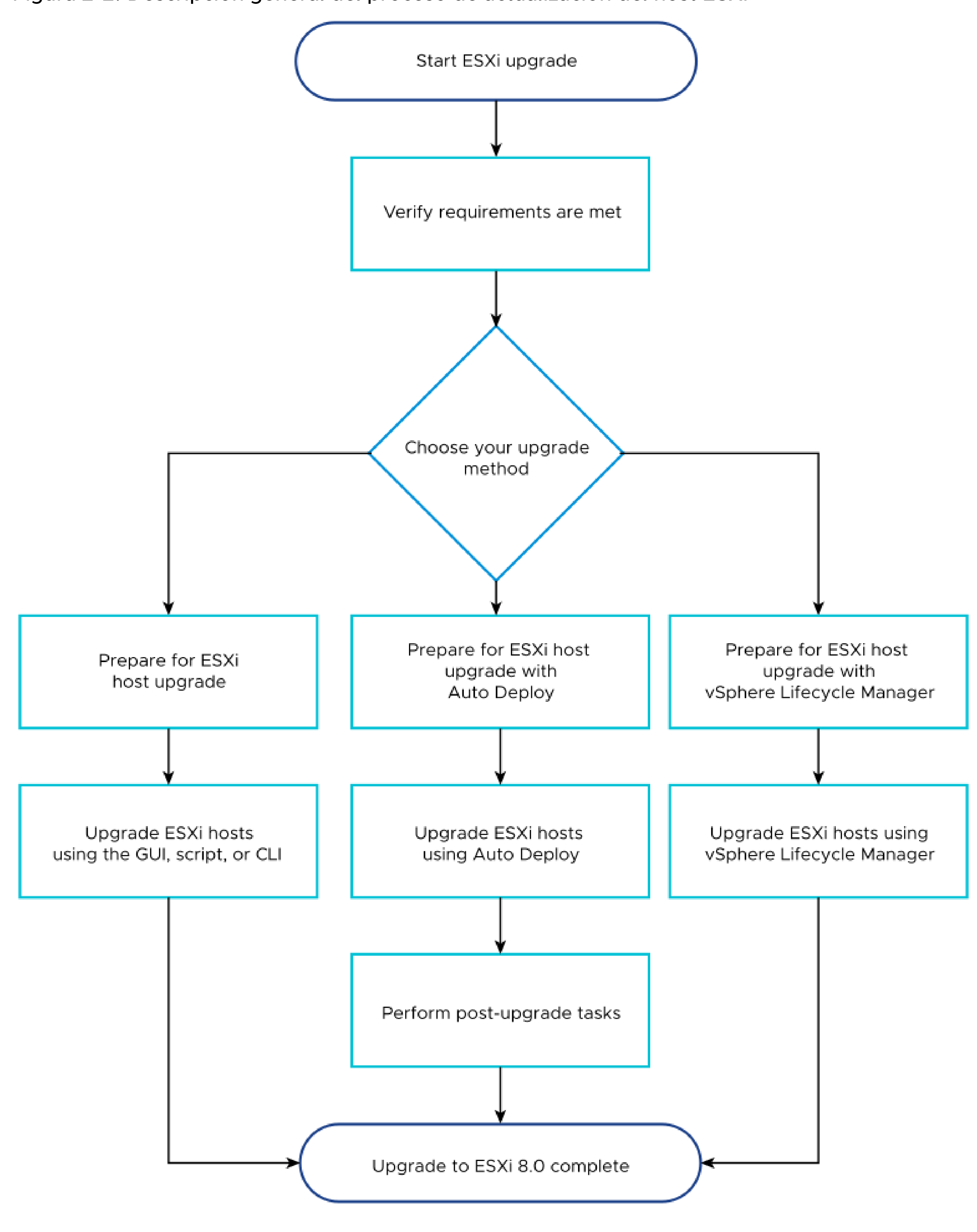
Descripción general del proceso de actualización del host ESXi

VMware ofrece varias maneras de actualizar hosts ESXi con versiones antiguas a la versión ESXi 8.0.

Los detalles y el nivel de compatibilidad para una actualización a ESXi 8.0 dependen del host que se desea actualizar y del método de actualización que se utiliza. Compruebe la compatibilidad de la ruta de acceso de actualización de su versión actual de ESXi a la versión a la cual desea actualizar. Para obtener más información, consulte las Matrices de interoperabilidad de productos de VMware en http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Puede actualizar un host ESXi a la versión 8.0 haciendo una actualización interactiva desde un CD, DVD o USB, una actualización generada por script, ESXCLI o vSphere Lifecycle Manager. Cuando se actualiza un host ESXi que tiene VIB personalizados a la versión 8.0, se migran todos los VIB personalizados compatibles. Para obtener más información, consulte Actualización de hosts con VIB personalizados de terceros.

Figura 2-2. Descripción general del proceso de actualización del host ESXi



Los siguientes pasos de alto nivel son para actualizar ESXi.

1 Compruebe que el sistema cumpla los requisitos de actualización. Consulte Requisitos de ESXi.

2 Prepare el entorno antes de llevar a cabo la actualización. Consulte Antes de actualizar los hosts ESXi.

3 Determine dónde desea ubicar y arrancar el instalador de ESXi. Consulte Opciones de medios para arrancar el instalador de ESXi. Si va a realizar un arranque de red del instalador, compruebe que la infraestructura de arranque de red esté configurada correctamente. Consulte Arranque de red del instalador de ESXi.

4 Actualice ESXi. Consulte Capítulo 3 Actualizar hosts ESXi

5 Después de actualizar los hosts ESXi, debe volver a conectarlos a vCenter Server y volver a aplicar las licencias. Consulte Después de actualizar hosts ESXi.

Se admiten los siguientes métodos para una actualización directa a ESXi 8.0.

- Utilizar el instalador interactivo de la interfaz gráfica de usuario (Graphical User Interface, GUI) a partir de un CD, un DVD o una unidad USB.
- Realizar una actualización generada por script.
- Utilizar ESXCLI.
- Use vSphere Auto Deploy. Si el host ESXi se implementa mediante vSphere Auto Deploy, se puede utilizar vSphere Auto Deploy para reaprovisionar el host con una imagen de 8.0.
- Utilice vSphere Lifecycle Manager.

Instalador de interfaz gráfica de usuario (GUI)

Puede actualizar de forma interactiva mediante una imagen ISO del instalador de ESXi en un CD, DVD o unidad flash USB, o bien mediante el arranque de red del instalador. Este método es adecuado para implementaciones con pocos hosts. Si, durante el proceso de instalación, selecciona un disco de destino que contiene una instalación de ESXi, el instalador actualiza el host a ESXi 8.0. El instalador también entrega la opción de migrar alguna configuración del host existente y archivos de configuración y de mantener el almacén de datos existente de VMFS. Consulte Actualizar hosts de forma interactiva.

Realizar una actualización generada por script

Para realizar una actualización generada por script, puede usar el instalador de ESXi 8.0 desde una unidad Flash de CD, DVD o USB, o bien mediante el arranque de red del instalador. Este método es una forma eficiente de implementar varios hosts. Para obtener más información, consulte Instalar o actualizar hosts mediante un script.

ESXCLI

Puede usar ESXCLI para actualizar hosts ESXi 6.7 o hosts ESXi 7.0 a hosts ESXi 8.0.

vSphere 8.0 incluye archivos de configuración, componentes, imágenes base y complementos como nuevas entregas de software que se pueden utilizar para actualizar o aplicar revisiones a hosts ESXi 8.0. Para obtener información sobre la administración de componentes, imágenes base y complementos en ESXi, consulte *Conceptos y ejemplos de ESXCLI*.

Para usar los comandos ESXCLI, debe instalar una instancia de ESXCLI independiente. Para obtener más información sobre la instalación y el uso de ESXCLI, consulte los siguientes documentos.

- *Introducción a ESXCLI*
- *Referencia de ESXCLI*

Consulte Actualizar los hosts a través de comandos ESXCLI .

vSphere Auto Deploy

Si se implementa un host ESXi con vSphere Auto Deploy, puede utilizar vSphere Auto Deploy para reaprovisionar el host y reiniciarlo con un nuevo perfil de imagen o una configuración que administre en un nivel de clúster. Un perfil de imagen contiene una actualización o una revisión de ESXi, un perfil de configuración de host y, de manera opcional, controladores o agentes de administración de terceros proporcionados por socios de VMware. Para agregar hosts ESXi a un clúster que administra la configuración de ESXi en un nivel de clúster, se crea una regla en Auto Deploy que asigna ese clúster como la ubicación de host para los hosts recién agregados, los cuales heredan la misma configuración y no requieren una configuración manual. Puede crear imágenes personalizadas utilizando vSphere ESXi Image Builder CLI. Para obtener más información, consulte Capítulo 4 Usar vSphere Auto Deploy para reaprovisionar hosts .

vSphere Lifecycle Manager

vSphere Lifecycle Manager es un servicio de vCenter Server para instalar y actualizar hosts ESXi. Mediante el uso de imágenes y líneas base, vSphere Lifecycle Manager permite la administración centralizada y simplificada del ciclo de vida para varios hosts ESXi en el nivel del clúster. Para obtener más información sobre cómo realizar instalaciones y actualizaciones organizadas, consulte la documentación de *Administración del ciclo de vida de hosts y clústeres*.

Actualizar máquinas virtuales y VMware Tools

Después de actualizar un hosts ESXi, puede actualizar las máquinas virtuales en el host para aprovechar las nuevas características.

Dispone de las siguientes herramientas para actualizar máquinas virtuales.

vSphere Client

Puede utilizar vSphere Client para actualizar una máquina virtual paso a paso. Para obtener información sobre cómo actualizar las máquinas virtuales, consulte la documentación de *Administrar máquinas virtuales de vSphere*.

vSphere Lifecycle Manager

Puede utilizar vSphere Lifecycle Manager para actualizar el hardware de la máquina virtual y las versiones de VMware Tools de las máquinas virtuales de su entorno. vSphere Lifecycle Manager automatiza el proceso de actualización y verifica que los pasos se produzcan

en el orden correcto. Para obtener más información, consulte la documentación sobre *Administración del ciclo de vida de hosts y clústeres*.

Actualizar hosts ESXi

3

Después de actualizar vCenter Server, debe actualizar los hosts ESXi. Puede actualizar los hosts ESXi 6.7 y 7.0 directamente a ESXi 8.0.

Para actualizar los hosts, puede utilizar las herramientas y los métodos descritos en Descripción general del proceso de actualización del host ESXi.

Precaución Si actualiza los hosts administrados por vCenter Server, primero debe actualizar vCenter Server antes de actualizar los hosts ESXi. Si no actualiza el entorno en el orden correcto, es posible que se pierdan datos y no se pueda acceder a los servidores.

Lea los siguientes temas a continuación:

- Requisitos de ESXi
- Antes de actualizar los hosts ESXi
- Actualización de hosts con VIB personalizados de terceros
- Actualizar hosts ESXi en un entorno con VMware NSX
- Opciones de medios para arrancar el instalador de ESXi
- Descarga del instalador de ESXi
- Identificadores y nombres de dispositivos de almacenamiento de ESXi
- Actualizar hosts de forma interactiva
- Instalar o actualizar hosts mediante un script
- Cómo arrancar un host ESXi desde un dispositivo de red
- Cómo actualizar hosts mediante comandos ESXCLI
- Después de actualizar hosts ESXi

Requisitos de ESXi

Para instalar o actualizar ESXi, el sistema debe cumplir con requisitos de hardware y software específicos.

Descripción general del almacenamiento del sistema ESXi

ESXi 8.0 tiene un diseño de almacenamiento del sistema que permite la administración flexible de particiones y componentes de terceros, a la vez que facilita la depuración.

Almacenamiento del sistema ESXi

El diseño del almacenamiento del sistema ESXi 8.0 consta de cuatro particiones:

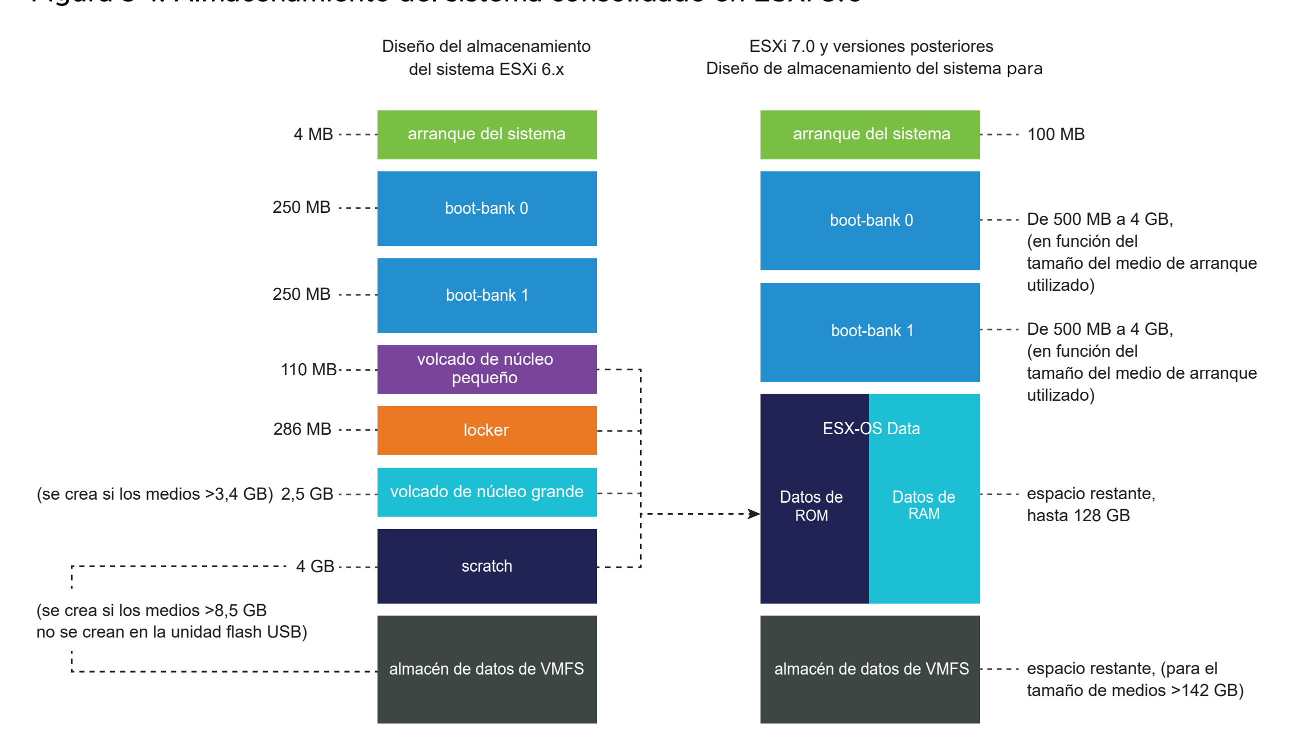
Tabla 3-1. particiones de almacenamiento del sistema ESXi:

Partición	Uso	Tipo
Arranque del sistema	Almacena el cargador de arranque y los módulos EFI.	FAT16
Boot-bank 0	Espacio del sistema destinado a almacenar los módulos de arranque de ESXi.	FAT16
Boot-bank 1	Espacio del sistema destinado a almacenar los módulos de arranque de ESXi.	FAT16
ESX-OSData	Actúa como la ubicación unificada para almacenar módulos adicionales. No se utiliza para los arranques ni las máquinas virtuales. Consolida la partición `/scratch` heredada, la partición del bloqueador para VMware Tools y los destinos de volcado de núcleo. **Precaución** En caso de que el medio de instalación sea un dispositivo de tarjeta SD o USB, la práctica recomendada es crear particiones ESX-OSData en un dispositivo de almacenamiento persistente que no se comparta entre hosts ESXi.	VMFS-L

El volumen ESX-OSData se divide en dos categorías de datos de alto nivel: datos persistentes y no persistentes. Los datos persistentes contienen datos que se escriben con poca frecuencia; por ejemplo, archivos ISO de VMware Tools, configuraciones y volcados de núcleo.

Los datos no persistentes contienen datos que se escriben con frecuencia; por ejemplo, registros, seguimientos globales de VMFS, datos del daemon de persistencia de entrada (Entry Persistence Daemon, EPD) de vSAN, seguimientos de vSAN y bases de datos en tiempo real.

Figura 3-1. Almacenamiento del sistema consolidado en ESXi 8.0



Tamaños del almacenamiento del sistema ESXi

A excepción de la partición de arranque del sistema, los tamaños de las particiones pueden variar en función del tamaño de los medios de arranque que se utilicen. Si el medio de arranque es de gran resistencia con una capacidad superior a 142 GB, se crea automáticamente un almacén de datos de VMFS para almacenar los datos de la máquina virtual.

Si desea revisar la capacidad de los medios de arranque y el ajuste de tamaño automático que configura el instalador de ESXi, utilice vSphere Client y vaya a la vista **Detalles de particiones**. Si lo prefiere, puede usar ESXCLI; por ejemplo, el comando `esxcli storage filesystem list`.

Tabla 3-2. Tamaños del almacenamiento del sistema ESXi en función del medio de arranque que se utilice y su capacidad

Tamaño del medio de arranque	8 a 10 GB	10 a 32 GB	32 a 128 GB	>128 GB
Arranque del sistema	100 MB	100 MB	100 MB	100 MB
Boot-bank 0	500 MB	1 GB	4 GB	4 GB
Boot-bank 1	500 MB	1 GB	4 GB	4 GB
ESX-OSData	espacio restante	espacio restante	espacio restante	hasta 128 GB
almacén de datos de VMFS				espacio restante para el tamaño de medios >142 GB

Se puede usar la opción de arranque del instalador de ESXi `systemMediaSize` para limitar el tamaño de las particiones de almacenamiento del sistema en el medio de arranque. Si el sistema tiene un espacio pequeño que no requiere el tamaño máximo de almacenamiento del sistema de 128 GB, puede limitarlo al mínimo de 32 GB. El parámetro `systemMediaSize` acepta los siguientes valores:

- min (32 GB, para servidores integrados o con un único disco)
- small (64 GB, para servidores con al menos 512 GB de RAM)
- default (128 GB)
- max (consumir todo el espacio disponible, para servidores de varios terabytes)

El valor seleccionado debe adecuarse al propósito del sistema. Por ejemplo, un sistema con 1 TB de memoria debe usar un mínimo de 64 GB para el almacenamiento del sistema. Para establecer la opción de arranque en el momento de la instalación (por ejemplo, `systemMediaSize=small`), consulte Introducir las opciones de arranque para iniciar un script de instalación o actualización. Para obtener más información, consulte el artículo 81166 de la base de conocimientos.

Vínculos del almacenamiento del sistema ESXi

Los subsistemas que requieren acceso a las particiones de ESXi acceden a estas particiones mediante los siguientes vínculos simbólicos:

Tabla 3-3. Vínculos simbólicos del almacenamiento del sistema ESXi

Volumen del almacenamiento del sistema	Vínculo simbólico
Boot-bank 0	`/bootbank`
Boot-bank 1	`/altbootbank`

Datos persistentes	`/productLocker`
	`/locker`
	`/var/core`
	`/usr/lib/vmware/isoimages`
	`/usr/lib/vmware/floppies`

Datos no persistentes	`/var/run`
	`/var/log`
	`/var/vmware`
	`/var/tmp`
	`/scratch`

Comportamiento de almacenamiento

Al iniciar ESXi, el host entra en una fase de autoconfiguración durante la que se configuran los dispositivos de almacenamiento del sistema con los valores predeterminados.

Cuando reinicie el host ESXi después de instalar la imagen de ESXi, el host configura los dispositivos de almacenamiento del sistema con la configuración predeterminada. A partir de ESXi 7.0, puede activar la opción `autoPartition`, la cual formatea automáticamente todos los dispositivos vacíos disponibles con VMFS, excepto los dispositivos SD y USB heredados. El valor predeterminado es `autoPartition=FALSE`, que formatea dispositivos de arranque solo con VMFS con un tamaño superior a 128 GB. Para obtener más información, consulte el artículo 77009 de la base de conocimientos de VMware.

Precaución ESXi sobrescribe cualquier disco que parezca estar vacío. Los discos se consideran vacíos si no poseen una tabla de particiones o particiones válidas. Si usa software que utiliza dichos discos, en particular si está utilizando un administrador de volúmenes lógicos (LVM) en lugar de o además de esquemas tradicionales de particionamiento, ESXi podría causar un reformateo del LVM local. Realice una copia de seguridad de los datos del sistema antes de habilitar ESXi por primera vez.

En el disco duro o dispositivo USB desde el que arranca el host ESXi, el software de formateo de discos conserva las particiones de diagnóstico existentes que el proveedor de hardware crea. En el espacio restante, el software crea las particiones descritas a continuación.

Particiones creadas por ESXi en la unidad del host

Para instalaciones nuevas, se crean varias particiones nuevas para el arranque del sistema, los bancos de arranque y ESX-OSData. La instalaciones desde cero de ESXi utilizan las tablas de particiones GUID (GPT) en lugar del particionamiento basado en MSDOS. El instalador crea bancos de arranque de diferentes tamaños en función del tamaño del disco. Para obtener más información sobre la partición desde cero, consulte Acerca de la partición desde cero.

El instalador afecta solamente al disco de instalación. El instalador no afecta a otros discos del servidor. Cuando se realiza la instalación en un disco, el instalador sobrescribe el disco completo. Cuando el instalador configura automáticamente el almacenamiento, no sobrescribe las particiones del proveedor de hardware.

Para crear el almacén de datos de VMFS, el instalador de ESXi necesita un mínimo de 128 GB de espacio disponible en el disco de instalación.

Es posible que desee anular este comportamiento predeterminado si, por ejemplo, utiliza dispositivos de almacenamiento compartido en lugar de almacenamiento local. A fin de evitar un formateo automático de discos, desconecte los dispositivos de almacenamiento local del host en las siguientes circunstancias:

- Antes de ejecutar el host por primera vez.
- Antes de ejecutar el host después de restablecerlo a los valores predeterminados de configuración.

Para anular el formateo VMFS, si ya se realizó el formateo automático de discos, puede eliminar el almacén de datos. Consulte la documentación de *Administrar vCenter Server y hosts*.

Acerca de la partición desde cero

En las instalaciones nuevas de ESXi, durante la fase de configuración automática, se crea una partición desde cero como parte de la partición ESX-OSDATA.

Nota La partición de hosts que se actualizan a ESXi 7.0 y versiones posteriores a partir de versiones anteriores varía de manera significativa respecto de la partición de las nuevas instalaciones de ESXi. El proceso de actualización a ESXi 7.0 y otras versiones posteriores vuelve a particionar el dispositivo de arranque y consolida el volcado de núcleo, el bloqueador y las particiones desde cero originales en el volumen ESX-OSData.

La partición desde cero se usa para almacenar registros del sistema que se necesitan cuando se crea un paquete de soporte. Si no hay ninguna partición desde cero, los registros del sistema se almacenan en un disco RAM. Si no se crea ninguna partición desde cero, puede configurar una. También puede anular la configuración predeterminada.

La partición desde cero se puede crear en un directorio remoto montado en SAN o NFS.

Establecer la partición desde cero de vSphere Client

Si no hay configurada ninguna partición desde cero, es posible que quiera configurar una, especialmente si el host tiene poca memoria. Cuando no hay ninguna partición desde cero, los registros del sistema se almacenan en un disco RAM.

Requisitos previos

El directorio que se usará para la partición temporal debe existir en el host.

Procedimiento

1. Desde vSphere Client, conéctese a vCenter Server.
2. Seleccione el host en el inventario.
3. Haga clic en la pestaña **Configurar**.
4. Seleccione **Sistema**.
5. Seleccione **Configuración avanzada del sistema**.

   El parámetro **ScratchConfig.CurrentScratchLocation** muestra la ubicación actual de la partición desde cero.
6. En el cuadro de texto **ScratchConfig.ConfiguredScratchLocation**, introduzca una ruta de acceso de directorio que sea exclusiva para este host.

   Por ejemplo, **`/vmfs/volumes/`*`DatastoreUUID`*`/`*`DatastoreFolder`***.
7. Reinicie el host para que se apliquen los cambios.

Requisitos de hardware de ESXi

Asegúrese de que el host cumpla la configuración de hardware mínima de ESXi8.0.

Recursos de hardware y del sistema

Para instalar o actualizar ESXi, los recursos de hardware y del sistema deben cumplir los siguientes requisitos:

- Plataforma de servidores compatible. Para obtener una lista de plataformas compatibles, consulte la *Guía de compatibilidad de VMware* en http://www.vmware.com/resources/compatibility.
- ESXi 8.0 requiere un host con al menos dos núcleos de CPU.
- ESXi 8.0 admite una amplia gama de procesadores x86 de 64 bits de varios núcleos. Para obtener una lista completa de procesadores compatibles, consulte la guía de compatibilidad de VMware en http://www.vmware.com/resources/compatibility.
- ESXi 8.0 requiere que el bit NX/XD esté habilitado para la CPU en el BIOS.
- ESXi 8.0 requiere un mínimo de 8 GB de RAM física. Proporcione al menos 12 GB de RAM para ejecutar máquinas virtuales en entornos de producción típicos.
- Para admitir máquinas virtuales de 64 bits, se debe habilitar la compatibilidad para virtualización de (Intel VT-x o RVI AMD) en CPU x64.
- Una o más controladoras Gigabit o Ethernet más rápidas. Para obtener una lista de modelos de adaptadores de red compatibles, consulte la *Guía de compatibilidad de VMware* en http://www.vmware.com/resources/compatibility.
- ESXi 8.0 requiere un disco de arranque de al menos 32 GB de almacenamiento persistente, como HDD, SSD o NVMe. No se debe compartir un dispositivo de arranque entre hosts ESXi.
- Disco SCSI o un LUN RAID local que no sea de red con espacio sin particionar para las máquinas virtuales.
- Para la serie ATA (SATA), un disco conectado a través de controladoras SAS compatibles o controladoras SATA integradas compatibles. Los discos SATA se consideran remotos, no locales. Estos discos no se usan como una partición desde cero de forma predeterminada, ya que se consideran remotos.

  Nota No puede conectar un dispositivo CD-ROM SATA a una máquina virtual en un host ESXi. Para usar el dispositivo CD-ROM SATA, debe usar el modo de emulación IDE.

Sistemas de almacenamiento

Para obtener una lista de sistemas de almacenamiento compatibles, consulte la *Guía de compatibilidad de VMware* en http://www.vmware.com/resources/compatibility. A partir de ESXi 8.0, no se pueden utilizar adaptadores de software para canal de fibra en Ethernet (Fibre Channel over Ethernet, FCoE), solo adaptadores de FCoE de hardware.

Requisitos de arranque de ESXi

En vSphere 8.0, la compatibilidad con BIOS heredado es limitada y se recomienda arrancar los hosts ESXi desde la Unified Extensible Firmware Interface (UEFI). Con la UEFI, puede arrancar sistemas desde unidades de disco duro, unidades de CD-ROM o medios USB. vSphere Auto Deploy admite el arranque de redes y el aprovisionamiento de hosts ESXi mediante UEFI. Si el sistema tiene unidades de procesamiento de datos (DPU) admitidas, solo puede usar UEFI para instalar y arrancar ESXi en las DPU. Para obtener más información sobre los planes de VMware para dejar de admitir BIOS heredado en plataformas de servidor, consulte el artículo https://kb.vmware.com/s/article/84233 de la base de conocimientos.

ESXi puede arrancar desde un disco con más de 2 TB siempre que el firmware del sistema y el firmware en cualquier tarjeta adicional que esté usando lo admitan. Consulte la documentación del proveedor.

Requisitos de almacenamiento para la instalación o actualización de ESXi 8.0

Para obtener el mejor rendimiento de una instalación de ESXi 8.0 utilice un dispositivo de almacenamiento persistente con un mínimo de 32 GB para los dispositivos de arranque. La actualización a ESXi 8.0 requiere un dispositivo de arranque de al menos 8 GB. Al arrancar desde un disco local, un LUN iSCSI o SAN, se necesita un disco de al menos 32 GB para permitir la creación de volúmenes de almacenamiento del sistema, incluida una partición de arranque, bancos de arranque y un volumen ESX-OSData basado en VMFS-L. El volumen ESX-OSData asume la función de la partición heredada `/scratch`, la partición de bloqueador para VMware Tools y el destino del volcado de núcleo.

Nota En ESXi 8.0, el volumen ESX-OSData se considera una partición unificada y los componentes independientes, como `/scratch` y VMware Tools, están consolidados en una sola partición persistente de OSDATA.

Otras opciones para obtener el mejor rendimiento de una instalación de ESXi 8.0 son las siguientes:

- Un disco local de 128 GB o más para ofrecer una compatibilidad óptima con ESX-OSData. El disco contiene la partición de arranque, el volumen ESX-OSData y un almacén de datos de VMFS.
- Un dispositivo que admite un mínimo de 128 Terabytes escritos (terabytes written, TBW).
- Un dispositivo que proporciona al menos 100 MB/s de velocidad de escritura secuencial.
- Para proporcionar resiliencia en caso de que se produzca un error en el dispositivo, se recomienda un dispositivo reflejado RAID 1.

Con las siguientes limitaciones, se admiten los dispositivos USB y SD heredados:

- Los dispositivos SD y USB se admite para las particiones de banco de arranque. El uso de dispositivos SD y USB para almacenar particiones ESX-OSData está obsoleto y la práctica recomendada consiste en proporcionar un dispositivo local persistente independiente con un

mínimo de 32 GB para almacenar el volumen ESX-OSData. El dispositivo de arranque local persistente puede ser un dispositivo flash M.2 de grado industrial (SLC y MLC), SAS, SATA, HDD, SSD o NVMe. La capacidad óptima para los dispositivos locales persistentes es de 128 GB.

- Si no proporciona almacenamiento persistente, verá una alarma del tipo `No se encontró ningún dispositivo persistente secundario. Mueva la instalación a almacenamiento persistente, ya que la compatibilidad con la configuración solo de tarjeta SD/USB va a dejar de utilizarse`.
- Debe utilizar un dispositivo flash SD aprobado por el proveedor del servidor para el modelo de servidor en particular en el que desea instalar ESXi en un dispositivo de almacenamiento flash SD. Puede encontrar una lista de dispositivos validados en partnerweb.vmware.com.
- Consulte el artículo de la base de conocimientos 85685 sobre las instrucciones actualizadas para entornos basados en tarjetas SD o USB.
- Para elegir un dispositivo de arranque SD o USB adecuado, consulte el artículo 82515 de la base de conocimientos.

El proceso de actualización a ESXi 8.0 desde versiones anteriores a la 7.x vuelve a particionar el dispositivo de arranque y consolida el volcado de núcleo, el bloqueador y las particiones scratch originales en el volumen ESX-OSData.

Los siguientes eventos se producen durante el proceso de reparticionamiento:

- Si no se configura un destino de volcado de núcleo personalizado, la ubicación predeterminada es un archivo en el volumen ESX-OSData.
- Si el servicio de syslog está configurado para almacenar archivos de registro en la partición temporal de VFAT de 4 GB, los archivos de registro de `var/run/log` se migran al volumen ESX-OSData.
- VMware Tools se migra de la partición del bloqueador y se borra la partición.
- Se elimina la partición de volcado de núcleo. Se eliminan los archivos de volcado de núcleo de la aplicación que se almacenan en la partición temporal.

Nota No es posible revertir de ESXi 8.x a una versión de ESXi anterior a la versión 7.x debido al proceso de nueva partición del dispositivo de arranque. Para utilizar una versión de ESXi anterior a la versión 7.x después de actualizar a la versión 8.0, debe crear una copia de seguridad del dispositivo de arranque antes de la actualización y restaurar el dispositivo de arranque de ESXi a partir de la copia de seguridad. La reversión de ESXi 8.x a 7.x es posible siempre que no se hayan realizado cambios en las particiones bootbank y no se detecte ninguna partición dañada.

Si utiliza dispositivos USB o SD para realizar una actualización, la práctica recomendada es asignar una región ESX-OSData en un disco persistente disponible o un LUN de SAN. Si no hay disponibles almacenamiento persistente o un LUN de SAN, ESX-OSData se crea automáticamente en un disco RAM. VMFS también se puede utilizar para la partición ESX-OSData.

Después de la actualización, si ESX-OSData reside en un disco RAM, un nuevo dispositivo persistente se encuentra en arranques posteriores y ese dispositivo tiene el ajuste `autoPartition=True`, ESX-OSData se crea automáticamente en el nuevo dispositivo persistente. ESX-OSData no se mueve automáticamente entre almacenamientos persistentes, pero es posible cambiar manualmente la ubicación de ESX-OSData a un almacenamiento compatible.

Para obtener más información sobre cómo volver a configurar la partición `/scratch`, consulte la documentación de *Instalar y configurar vCenter Server*.

Para configurar el tamaño de las particiones del sistema ESXi, puede utilizar la opción `systemMediaSize`. Para obtener más información, consulte el artículo https://kb.vmware.com/s/article/81166 de la base de conocimientos.

En instalaciones de Auto Deploy, el instalador intenta asignar una región temporal en un disco o un almacén de datos local disponible. Si no se encuentra ningún disco o almacén de datos local, se producirá un error en la instalación.

En los entornos que arrancan desde una SAN o utilizan Auto Deploy, el volumen ESX-OSData para cada host ESXi debe configurarse en un LUN de SAN separado.

Usar aplicaciones de administración remota

Las aplicaciones de administración remota permiten instalar ESXi en servidores que se encuentran en ubicaciones remotas.

Las aplicaciones de administración remota compatibles para la instalación incluyen HP Integrated Lights-Out (iLO), Dell Remote Access Card (DRAC), IBM management module (MM) y Remote Supervisor Adapter II (RSA II). Para obtener soporte técnico para las aplicaciones de administración remota, póngase en contacto con el proveedor.

Puede usar aplicaciones de administración remota para realizar instalaciones interactivas y por script de ESXi de forma remota.

Si utiliza aplicaciones de administración remota para instalar ESXi, el CD virtual podría encontrarse con daños en sistemas o redes que operan a capacidad máxima. Si se produce un error en una instalación remota de una imagen ISO, complete la instalación desde el CD físico.

Modelos de servidores de administración remota compatibles y versiones de firmware

Puede utilizar aplicaciones de administración remota para instalar o actualizar ESXi o para administrar hosts de forma remota.

Tabla 3-4. Modelos de servidores de administración remota compatibles y versiones de firmware mínimas

Modelo de servidor de administración remota	Versión de firmware	Java
Dell DRAC 9	6.0.30.00	N/C
Dell DRAC 7	1.30.30 (compilación 43)	1.7.0_60-b19
Dell DRAC 6	1.54 (compilación 15), 1.70 (compilación 21)	1.6.0_24
Dell DRAC 5	1.0, 1.45, 1.51	1.6.0_20,1.6.0_203
Dell DRAC 4	1.75	1.6.0_23
ILO HP	1.81, 1.92	1.6.0_22, 1.6.0_23
ILO HP 2	1.8, 1.81	1.6.0_20, 1.6.0_23
ILO HP 3	1.28	1.7.0_60-b19
ILO HP 4	1.13	1.7.0_60-b19
ILO HP 5	2.72	N/C
RSA IBM 2	1.03, 1.2	1.6.0_22

Recomendaciones para un rendimiento mejorado de ESXi

Para mejorar el rendimiento, instale o actualice ESXi en un sistema robusto con más RAM que el mínimo necesario y con varios discos físicos.

Para conocer los requisitos del sistema de ESXi, consulte Requisitos de hardware de ESXi.

Tabla 3-5. Recomendaciones para un mejor rendimiento

Elemento del sistema	Recomendación
RAM	Los hosts ESXi requieren más RAM que los servidores típicos. ESXi 8.0 requiere un mínimo de 8 GB de RAM física. Proporcione al menos 12 GB de RAM para aprovechar al máximo las características de ESXi y ejecutar máquinas virtuales en entornos de producción típicos. Un host ESXi debe tener suficiente RAM para que funcionen máquinas virtuales simultáneas. Se proporcionan los siguientes ejemplos para ayudar a calcular la RAM que necesitan las máquinas virtuales que se ejecutan en el host ESXi. Para operar cuatro máquinas virtuales con Red Hat Enterprise Linux o Windows XP se requiere al menos 3 GB de RAM para rendimiento línea base. Esta cifra incluye 1.024 MB para las máquinas virtuales, 256 MB como mínimo para cada sistema operativo, según lo que recomiendan los proveedores. Para que estas cuatro máquinas virtuales funcionen con 512 MB de RAM, es necesario que los hosts ESXi tengan 4 GB de RAM, lo que incluye 2.048 MB para las máquinas virtuales. Estos cálculos no incluyen los posibles ahorros de memoria derivados de usar memoria con sobrecarga variable para cada máquina virtual. Consulte *Administración de recursos de vSphere*.
Adaptadores Fast Ethernet dedicados para máquinas virtuales	Coloque la red de administración y las redes de máquinas virtuales en tarjetas de red físicas distintas. Las tarjetas Gigabit Ethernet dedicadas para máquinas virtuales, como adaptadores Intel PRO 1000, mejoran el rendimiento para máquinas virtuales con gran tráfico de red.
Ubicación del disco	Coloque todos los datos que usan las máquinas virtuales en discos físicos asignados específicamente a máquinas virtuales. El rendimiento es mejor cuando no coloca las máquinas virtuales en el disco que contiene la imagen de arranque de ESXi. Use discos físicos que sean lo bastante grandes para mantener imágenes del disco que usan todas las máquinas virtuales.
Partición de VMFS6	El instalador de ESXi crea los volúmenes iniciales de VMFS en el primer disco local en blanco que se encuentra. Para agregar discos o modificar la configuración original, use vSphere Client. Esta práctica asegura que los sectores de arranque de las particiones estén alineados con 64K, lo que mejora el rendimiento del almacenamiento. **Nota** Para entornos únicamente de SAS, es posible que el instalador no formatee los discos. Para algunos discos SAS, no es posible identificar si los discos son locales o remotos. Después de la instalación, se puede usar vSphere Client para configurar VMFS.

Tabla 3-5. Recomendaciones para un mejor rendimiento (continuación)

Elemento del sistema	Recomendación
Procesadores	Los procesadores más rápidos mejoran el rendimiento de ESXi. Para ciertas cargas de trabajo, una mayor cantidad de memorias caché mejoran el rendimiento de ESXi.
Compatibilidad de hardware	Use dispositivos en el servidor que sean compatibles con controladores de ESXi. Consulte la *Guía de compatibilidad de hardware* en http://www.vmware.com/resources/compatibility.

Puertos de firewall entrantes y salientes para hosts de ESXi

Abra y cierre los puertos de firewall de cada servicio mediante vSphere Client o VMware Host Client.

ESXi incluye un firewall que está habilitado de forma predeterminada. En el momento de realizar la instalación, el firewall de ESXi se configura para bloquear el tráfico entrante y saliente, excepto el tráfico de los servicios que están habilitados en el perfil de seguridad del host. Para obtener la lista de los puertos y protocolos compatibles en el firewall de ESXi, consulte la herramienta VMware Ports and Protocols™ en https://ports.vmware.com/.

La herramienta VMware Ports and Protocols muestra la información sobre los puertos de los servicios que se instalan de forma predeterminada. Si instala otros VIB en el host, es posible que estén disponibles otros puertos de firewall y servicios adicionales. La información es principalmente para los servicios que están visibles en vSphere Client, pero la herramienta VMware Ports and Protocols también incluye otros puertos.

Espacio libre necesario para registro del sistema

Consulte la configuración recomendada de tamaño y rotación mínima para registros hostd, vpxa y fdm.

Si utilizó Auto Deploy para instalar el host ESXi 8.0 o bien si configuró un directorio de registro separado de la ubicación predeterminada en un directorio totalmente nuevo en el volumen de VMFS, es posible que deba cambiar su configuración de tamaño y rotación de registro actual para garantizar que el espacio disponible sea suficiente para el registro del sistema. Todos los componentes de vSphere usan esta infraestructura. Los valores predeterminados para la capacidad de registros en esta infraestructura varían según la cantidad de almacenamiento disponible y cómo ha configurado el registro del sistema. Los hosts que se implementan con Auto Deploy almacenan registros en un disco RAM, lo que significa que hay poca cantidad de espacio disponible para registros.

Si su host se implementa con Auto Deploy, vuelva a configurar el almacenamiento de sus registros de una de estas formas:

- Redirija los registros a través de la red hacia un recopilador remoto.
- Redirija registros hacia un almacenamiento NAS o NFS.

Si redirige los registros hacia un almacenamiento no predeterminado, como NAS o NFS, es posible que también desee volver a configurar el dimensionamiento y las rotaciones de los registros para los hosts que están instalados en el disco.

No tiene que volver a configurar el almacenamiento de registros para hosts ESXi que utilizan la configuración predeterminada, que almacena registros en un directorio temporal en el volumen de VMFS. Para estos hosts, ESXi 8.0 configura registros que se adapten de la mejor manera a cada instalación y proporciona suficiente espacio para alojar mensajes de registros.

Tabla 3-6. Configuración recomendada de tamaño y rotación mínima para registros hostd, vpxa y fdm

Registro	Tamaño máximo de archivo de registro	Número de archivos de registro que se van a conservar	Espacio de disco mínimo necesario
Agente de administración (hostd)	10 MB	10	100 MB
Agente VirtualCenter (vpxa)	5 MB	10	50 MB
Agente de vSphere HA (administrador de dominio de fallas, fdm)	5 MB	10	50 MB

De manera opcional, puede instalar VMware vCenter Log Insight, que brinda agregado y análisis de registros.

Requisitos del sistema de VMware Host Client

Asegúrese de que su explorador sea compatible con VMware Host Client.

Los siguientes sistemas operativos invitados y las siguientes versiones de exploradores web son compatibles con VMware Host Client.

Exploradores compatibles	Mac OS	Windows de 32 bits y 64 bits	Linux
Google Chrome	89+	89+	75+
Mozilla Firefox	80+	80+	60+
Microsoft Edge	90+	90+	N/C
Safari	9.0+	N/C	N/C

Bloqueo de cuenta y contraseñas ESXi

Para los hosts ESXi, debe utilizar una contraseña con requisitos predefinidos. Puede cambiar el requisito de longitud requerida y la clase de caracteres o permitir frases de contraseña si utiliza el ajuste del sistema avanzado `Security.PasswordQualityControl`. También puede establecer el

número de contraseñas para recordar para cada usuario mediante el ajuste del sistema avanzado `Security.PasswordHistory`.

Nota Los requisitos predeterminados para las contraseñas de ESXi pueden cambiar de una versión a otra. Puede comprobar las restricciones predeterminadas para la contraseña y modificarlas con el ajuste del sistema avanzado `Security.PasswordQualityControl`.

Contraseñas de ESXi

ESXi aplica requisitos de contraseña para el acceso desde la interfaz de usuario de la consola directa, ESXi Shell, SSH o VMware Host Client.

- De manera predeterminada, debe incluir una combinación de al menos tres de las cuatro clases de caracteres siguientes: letras en minúscula, letras en mayúscula, números y caracteres especiales, como el guion bajo o el guion, al crear una contraseña.
- De forma predeterminada, la longitud de la contraseña debe tener como mínimo 7 caracteres y menos de 40.
- Las contraseñas no deben contener una palabra de diccionario ni parte de una palabra de diccionario.
- Las contraseñas no deben contener el nombre de usuario ni partes del mismo.

Nota Un carácter en mayúscula al inicio de una contraseña no se tiene en cuenta en la cantidad de clases de caracteres que se utilizan. Un número al final de una contraseña no se tiene en cuenta en la cantidad de clases de caracteres que se utilizan. Una palabra del diccionario que se utiliza dentro de una contraseña reduce la longitud general de la contraseña.

Ejemplos de contraseñas de ESXi

A continuación se indican posibles contraseñas en caso de configurar la opción de la siguiente manera.

```
retry=3 min=disabled,disabled,disabled,7,7
```

Con esta opción, se solicita al usuario hasta tres veces (retry=3) una contraseña nueva si no es lo suficientemente segura o si la contraseña no se introdujo correctamente dos veces. No se permiten las contraseñas que tienen una o dos clases de caracteres ni las frases de contraseña, ya que los primeros tres elementos están desactivados. Las contraseñas de tres y cuatro clases de caracteres requieren siete caracteres. Consulte la página del manual de `pam_passwdqc` para obtener más información sobre otras opciones, como `max` y `passphrase`, entre otras.

Con esta configuración, se permiten las siguientes contraseñas.

- xQaTEhb!: contiene ocho caracteres de tres clases.
- xQaT3#A: contiene siete caracteres de cuatro clases.

Las siguientes contraseñas posibles no cumplen con los requisitos.

- Xqat3hi: comienza con un carácter en mayúscula, lo que reduce la cantidad efectiva de clases de caracteres a dos. La cantidad mínima de clases de caracteres requerida es tres.
- xQaTEh2: termina con un número, lo que reduce la cantidad efectiva de clases de caracteres a dos. La cantidad mínima de clases de caracteres requerida es tres.

Frase de contraseña de ESXi

En lugar de una contraseña, también puede utilizar una frase de contraseña. Sin embargo, las frases de contraseña están desactivadas de forma predeterminada. Puede cambiar este valor predeterminado u otros valores de configuración mediante el ajuste del sistema avanzado `Security.PasswordQualityControl` de vSphere Client.

Por ejemplo, puede cambiar la opción por la siguiente.

```
retry=3 min=disabled,disabled,16,7,7
```

Este ejemplo permite frases de contraseña de al menos 16 caracteres y al menos tres palabras.

En el caso de los hosts heredados, aún es posible cambiar el archivo `/etc/pam.d/passwd`, pero no se podrá hacer en las próximas versiones. Use el ajuste del sistema avanzado `Security.PasswordQualityControl` en su lugar.

Modificar las restricciones predeterminadas de contraseña

Puede cambiar la restricción predeterminada de contraseñas y frases de contraseña con el ajuste del sistema avanzado `Security.PasswordQualityControl` para su host ESXi. Consulte la documentación de *Administrar vCenter Server y hosts* para obtener información sobre cómo cambiar los ajustes avanzados del sistema de ESXi.

Puede cambiar el valor predeterminado, por ejemplo, para requerir un mínimo de 15 caracteres y una cantidad mínima de cuatro palabras (`passphrase=4`) de la siguiente manera:

```
retry=3 min=disabled,disabled,15,7,7 passphrase=4
```

Para obtener más información, consulte la página del manual de `pam_passwdqc`.

Nota Aún no se han probado todas las combinaciones posibles de opciones de contraseña. Después de cambiar la configuración de contraseña predeterminada, realice una prueba adicional.

En este ejemplo, se establece el requisito de complejidad de contraseña para requerir ocho caracteres de cuatro clases que aplican una diferencia significativa de contraseñas, un historial recordado de cinco contraseñas y una directiva de rotación de 90 días:

```
min=disabled,disabled,disabled,disabled,8 similar=deny
```

Comportamiento del bloqueo de cuentas de ESXi

Se admite el bloqueo de cuentas para el acceso a través de SSH y vSphere Web Services SDK. La interfaz de la consola directa (DCUI) y ESXi Shell no admiten el bloqueo de cuentas. De forma predeterminada, se permite un máximo de cinco intentos con errores antes de que la cuenta se bloquee. De forma predeterminada, la cuenta se desbloquea después de 15 minutos.

Configurar el comportamiento de inicio de sesión

Puede configurar el comportamiento de inicio de sesión del host ESXi con los siguientes ajustes del sistema avanzados:

- `Security.AccountLockFailures`. Cantidad máxima de intentos de inicio de sesión con errores antes de que la cuenta de un usuario se bloquee. Cero desactiva el bloqueo de cuentas.
- `Security.AccountUnlockTime`. Cantidad de segundos en los que el usuario queda bloqueado.
- `Security.PasswordHistory`. Número de contraseñas que se deben recordar para cada usuario. A partir de vSphere 8.0 Update 1, el valor predeterminado es cinco. Cero desactiva el historial de contraseñas.

Consulte la documentación de *Administrar vCenter Server y hosts* para obtener información sobre la configuración de las opciones avanzadas de ESXi.

Antes de actualizar los hosts ESXi

Para una actualización correcta de los hosts ESXi, comprenda y prepárese para los cambios que ello implica.

Para lograr una actualización satisfactoria de ESXi, siga estas prácticas recomendadas:

1 Asegúrese de comprender el proceso de actualización de ESXi, el efecto de dicho proceso en la implementación actual y la preparación necesaria para la actualización.

   - Si su sistema vSphere incluye soluciones o complementos de VMware, asegúrese de que sean compatibles con la versión de vCenter Server a la que va a actualizar. Consulte la matriz de interoperabilidad de productos de VMware en http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.
   - Lea Descripción general del proceso de actualización del host ESXi para comprender los escenarios de actualización que se admiten y, asimismo, las opciones y las herramientas que están disponibles para la realización de la actualización.
   - Lea las Notas de la versión de VMware vSphere para obtener información sobre los problemas de instalación conocidos.

2 Prepare el sistema para la actualización.

   - Asegúrese de que la versión actual de ESXi sea compatible con la actualización. Consulte Descripción general del proceso de actualización del host ESXi.
   - Asegúrese de que el hardware del sistema cumpla con los requisitos de ESXi. Consulte Requisitos de ESXi y la guía de compatibilidad de VMware en http://

www.vmware.com/resources/compatibility/search.php. Compruebe la compatibilidad del sistema, la compatibilidad de E/S con la red y las tarjetas de adaptador de bus host (HBA), la compatibilidad de almacenamiento y la compatibilidad del software de copia de seguridad.

- Asegúrese de que haya espacio en disco suficiente disponible en el host para la actualización.
- Si hay una SAN conectada al host, desconecte el sistema de canal de fibra antes de continuar con la actualización. No desactive las tarjetas HBA en el BIOS.

3 Cree una copia de seguridad del host antes de realizar una actualización. Si se produce un error en la actualización, puede restaurar el host.

4 Si utiliza Auto Deploy para aprovisionar hosts, el usuario que ejecuta el proceso debe tener privilegios de administrador local en el host ESXi que se aprovisiona. De manera predeterminada, el proceso de instalación tiene estos privilegios, y el aprovisionamiento de certificados se lleva a cabo según lo esperado. Sin embargo, si utiliza un método distinto al instalador, debe ejecutarlo como usuario con privilegios de administrador local.

5 Según la opción de actualización que elija, es posible que deba migrar o apagar todas las máquinas virtuales en el host. Consulte las instrucciones correspondientes para el método de actualización.

- Para una actualización interactiva desde CD, DVD o unidad USB, consulte Actualizar hosts de forma interactiva.
- Para una actualización generada por script, consulte Instalar o actualizar hosts mediante un script.
- Para vSphere Auto Deploy: consulte Capítulo 4 Usar vSphere Auto Deploy para reaprovisionar hosts . Si el host ESXi 6.7x o 7.0.x se implementó mediante vSphere Auto Deploy, se puede utilizar vSphere Auto Deploy para reaprovisionar el host con una imagen de 8.0.
- Para el método de comando `esxcli`: consulte Actualizar los hosts a través de comandos ESXCLI .

6 Planifique las tareas que deben realizarse después de la actualización del host ESXi:

- Pruebe el sistema para asegurarse de que la actualización se haya ejecutado correctamente.
- Aplique las licencias de un host. Consulte Licencias para hosts ESXi tras la actualización.
- Considere la posibilidad de configurar un servidor de Syslog para inicio de sesión remoto, a fin de garantizar que haya almacenamiento de disco suficiente para los archivos de registro. La configuración del registro en un host remoto es especialmente importante para hosts con almacenamiento local limitado. De manera opcional, puede instalar VMware vCenter Log Insight, que brinda agregado y análisis de registros. Consulte Espacio libre necesario para registro del sistema.

7 Si se produjo un error en la actualización y ha creado una copia de seguridad del host, puede restaurar el host.

Actualización de hosts con VIB personalizados de terceros

Un host puede tener paquetes de instalación de vSphere (VIB) personalizados instalados; por ejemplo, agentes de administración o controladores de otros fabricantes.

Cuando se actualiza un host ESXi a 8.0, se migran todos los VIB personalizados compatibles, independientemente de si los VIB se incluyen en el archivo ISO del instalador. Si el host o la imagen ISO del instalador contienen un VIB que genera un conflicto e impide la actualización, un mensaje de error identifica el VIB que generó el conflicto. Para actualizar el host, realice una de estas acciones:

- Quite el VIB que generó el conflicto del host ESXi y vuelva a intentar ejecutar la actualización. Puede eliminar un VIB del host mediante el uso de comandos de `esxcli`. Para obtener más información, consulte Quitar VIB de un host .
- Use vSphere ESXi Image Builder CLI para crear una imagen ISO personalizada de instalador que solucione el conflicto. Para obtener más información sobre vSphere ESXi Image Builder CLI, consulte la documentación de *Instalar y configurar vCenter Server*.

Actualizar hosts ESXi en un entorno con VMware NSX

En una configuración de VMware NSX, antes de actualizar a ESXi 8.0 y versiones posteriores, asegúrese de que el módulo de kernel de NSX forme parte de la línea base de imagen o actualización.

Si su sistema vSphere incluye VMware NSX, antes de iniciar una actualización de los hosts ESXi debe asegurarse de que el módulo de kernel de NSX forma parte de la línea base o de la especificación de software deseada que use para la actualización. Cuando se actualiza un host ESXi a la versión 8.0 o posterior, se migran todos los VIB personalizados compatibles, independientemente de si los VIB están incluidos en el archivo ISO del instalador. Sin embargo, el módulo de kernel de NSX no se migra automáticamente a la imagen ISO del instalador. Antes de continuar con la operación de actualización, debe realizar una de las siguientes acciones:

- Cree una línea base de extensión con un módulo de kernel de NSX recién cargado. Para obtener más información, consulte Administrar el ciclo de vida de clústeres y hosts.
- Cree un perfil de imagen personalizado con el módulo de kernel de NSX. Para obtener más información, consulte Actualizar ESXi mediante un perfil de imagen personalizado en una configuración de VMware NSX.
- Utilice PowerCLI para crear una nueva imagen ISO. Para obtener más información, consulte Actualizar ESXi en una configuración de VMware NSX con una nueva imagen ISO.
- Utilice ESXCLI. Para obtener más información, consulte Usar ESXCLI para actualizar hosts ESXi en una configuración VMware NSX.

Actualizar ESXi mediante un perfil de imagen personalizado en una configuración de VMware NSX

En una configuración de VMware NSX, antes de actualizar a ESXi 8.0 y versiones posteriores, asegúrese de que el módulo kernel de NSX forme parte de la línea base de actualización.

Requisitos previos

Si el sistema vSphere incluye VMware NSX, antes de iniciar una actualización de los hosts ESXi a 8.0 y versiones posteriores desde una versión anterior de ESXi, debe asegurarse de que el módulo de kernel de NSX forme parte de la línea base que se utiliza para la actualización. Para ello, puede crear un perfil de imagen personalizado con una imagen base ESXi y un módulo de kernel de NSX que acaba de cargar.

- Descargue de VMware Customer Connect el archivo ZIP del `módulo de kernel de NSX para VMware ESXi 8.0` para la versión de VMware NSX implementada en su entorno. Por ejemplo, `nsx-lcp-4.0.1.0.0.xxx-esx80.zip` para VMware NSX 4.0.1.
- Asegúrese de que Auto Deploy e Image Builder estén habilitados en su sistema vCenter Server.

Procedimiento

1 Inicie sesión en un sistema vCenter Server 8.x.

2 Acceda a **Inicio > Autodeploy > Almacenes de software** para importar al inventario de vSphere ESXi Image Builder una imagen base de ESXi 8.x, si aún no está disponible, y el archivo ZIP del módulo de kernel de NSX.

3 Cree un perfil de imagen que combine el módulo de kernel de VMware NSX y la imagen base para ESX 8.x. Para obtener pasos detallados, consulte Crear un perfil de imagen.

4 Exporte el perfil de imagen personalizado a una imagen ISO.

5 Importe la imagen ISO al almacén de vSphere Lifecycle Manager.

   Ahora puede crear una línea base de actualización basada en la imagen ISO importada mediante vSphere Lifecycle Manager. Para obtener más información acerca del flujo de trabajo de las actualizaciones de vSphere Lifecycle Manager con líneas base, consulte la guía Administrar el ciclo de vida de clústeres y hosts.

Actualizar ESXi en una configuración de VMware NSX con una nueva imagen ISO

En una configuración de VMware NSX, antes de actualizar a ESXi 8.0 y versiones posteriores, asegúrese de que el módulo de kernel de NSX forme parte de la línea base de imagen o actualización.

Requisitos previos

Si el sistema vSphere incluye VMware NSX, antes de iniciar una actualización de los hosts ESXi a 8.0 y versiones posteriores desde una versión anterior de ESXi, debe asegurarse de que el módulo de kernel de NSX forme parte de la especificación de software o línea base que se utiliza para la actualización. Para ello, puede usar el cmdlet `New-IsoImage` de PowerCLI para crear una nueva imagen ISO y realizar la actualización de ESXi del modo que prefiera.

- Descargue de VMware Customer Connect el archivo ZIP del `módulo de kernel de NSX para VMware ESXi 8.0` para la versión de VMware NSX implementada en su entorno. Por ejemplo, `nsx-lcp-4.0.1.0.0.xxx-esx80.zip` para VMware NSX 4.0.1.
- Instale el PowerCLI y todo el software necesario como requisito previo. Consulte Instalar y usar vSphere ESXi Image Builder.
- Compruebe que tiene acceso al almacén de software que contiene la especificación de software que desea utilizar.

Procedimiento

- ◆ En una sesión de PowerCLI, ejecute el cmdlet `New-IsoImage` para generar una imagen ISO pasando los parámetros `Depots`, `Destination` y `SoftwareSpec`. Por ejemplo, `PS C:\Users\Administrator> New-IsoImage -Depots "C:\VMware-ESXi-8.x.x-xxx-depot.zip","C:\nsx-lcp-4.0.1.0.0.xxx-esx80.zip", -Destination C:\<your new ISO image name>.iso -SoftwareSpec C:\<your file name>.json`. Este comando crea una nueva imagen ISO mediante la imagen base de ESXi y los archivos ZIP del kernel de NSX, además de la especificación de software de la imagen deseada en un archivo JSON. Puede usar cualquier número y combinación de almacenes de software, sin conexión y en línea. Para las actualizaciones a ESXi 8.0, el cmdlet `New-IsoImage` conserva los metadatos adicionales para ESXi 8.0 requeridos por el vSphere Lifecycle Manager.

Pasos siguientes

Utilice la nueva imagen ISO para completar la actualización de ESXi que prefiera. Para obtener más información acerca de los flujos de trabajo de las actualizaciones de vSphere Lifecycle Manager, consulte la guía Administrar el ciclo de vida de clústeres y hosts.

Usar ESXCLI para actualizar hosts ESXi en una configuración VMware NSX

En una configuración de VMware NSX, antes de actualizar a ESXi 8.0 y versiones posteriores, asegúrese de que el módulo de kernel de NSX forme parte de la línea base de imagen o actualización.

Si desea utilizar ESXCLI para actualizar un host ESXi en un sistema vSphere que incluye NSX-T Data Center, debe seguir los procedimientos descritos en Actualización de hosts mediante comandos ESXCLI:

Requisitos previos

Si el sistema vSphere incluye VMware NSX, antes de iniciar una actualización de los hosts ESXi a 8.0 y versiones posteriores desde una versión anterior de ESXi, debe asegurarse de que el módulo de kernel de NSX forme parte de la especificación de software o línea base que se utiliza para la actualización. Puede utilizar comandos ESXCLI para actualizar los hosts ESXi y volver a instalar el módulo de kernel de NSX.

- Descargue de VMware Customer Connect el archivo ZIP del `módulo de kernel de NSX para VMware ESXi 8.0` para la versión de VMware NSX implementada en su entorno. Por ejemplo, `nsx-lcp-4.0.1.0.0.xxx-esx80.zip` para VMware NSX 4.0.1.

Procedimiento

1 Coloque el host ESXi en modo de mantenimiento. Para obtener más información, consulte Colocar un host en modo de mantenimiento.

2 Descargue un perfil de imagen ESXi 8.x en un depósito de software accesible a través de una URL o en un almacén de archivos ZIP sin conexión.

3 Ejecute el comando ESXCLI `esxcli software profile update --depot <path-to-depot-file> -p ESXi-X.X.X-XXXXXX-standard --allow-downgrades --no-sig-check`. Por ejemplo: `esxcli software profile update --depot /vmfs/volumes/5e8fd197-68bce4dc-f8f1-005056af93cf/VMware-ESXi-8.0.0-xxx-depot.zip -p ESXi-8.0.0-xxx-standard --allow-downgrades --no-sig-check`. Para obtener más información, consulte Actualizar un host con perfiles de imagen.

4 Instale el módulo de kernel de NSX mediante el comando ESXCLI `esxcli software vib install -d <path_to_kernel_module_file> --no-sig-check`. Por ejemplo: `esxcli software vib install -d /tmp/nsx-lcp-4.0.1.0.0.xxx-esx80.zip`

5 Reinicie el host ESXi.

6 Quite el host ESXi del modo de mantenimiento.

Opciones de medios para arrancar el instalador de ESXi

El instalador de ESXi debe ser accesible para el sistema en el que se va a instalar ESXi.

Los siguientes medios de arranque son compatibles con el instalador de ESXi:

- Arranque desde un CD/DVD. Consulte Descargar y grabar un CD or DVD de la imagen ISO del instalador de ESXi.
- Arranque desde una unidad flash USB. Consulte Formatear una unidad flash USB para arrancar la instalación o la actualización de ESXi.
- Arranque desde una red. Consulte Arranque de red del programa de instalación de ESXi.
- Arranque desde una ubicación remota mediante una aplicación de administración remota. Consulte Usar aplicaciones de administración remota.

Descargar y grabar un CD or DVD de la imagen ISO del instalador de ESXi

Si no tiene un CD/DVD de instalación de ESXi, puede crear uno.

También puede crear una imagen ISO del instalador que incluya un script de instalación personalizado. Consulte Crear una imagen ISO de instalador con un script de instalación o actualización personalizado.

Procedimiento

1 Siga el procedimiento descrito en Descarga del instalador de ESXi.

2 Grabe la imagen ISO en un CD o DVD.

Formatear una unidad flash USB para arrancar la instalación o la actualización de ESXi

Puede formatear una unidad flash USB para arrancar la instalación o la actualización de ESXi.

En las instrucciones de este procedimiento se supone que la unidad flash USB se detecta como `/dev/sdb`.

Nota El archivo `ks.cfg` que contiene el script de instalación no puede estar ubicado en la misma unidad flash USB que se utiliza para arrancar la instalación o la actualización. El archivo kickstart no depende del arranque BIOS o UEFI.

Requisitos previos

- Equipo Linux al que se acceda como superusuario
- Unidad flash USB que el equipo Linux pueda detectar
- La imagen ISO de ESXi, `VMware-VMvisor-Installer-`*`número_de_versión-número_de_compilación`*`.x86_64.iso`, que incluye el archivo `isolinux.cfg`

Procedimiento

1 Arranque Linux, inicie sesión e introduzca el modo de superusuario mediante un comando `su` o `sudo root`.

2 Si la unidad flash USB no se detecta como `/dev/sdb`, o si no conoce con certeza la forma en que se detecta la unidad flash USB, determine la manera en que se detecta.

   a Conecte la unidad flash USB.

   b En la línea de comandos, ejecute el comando para mostrar los mensajes de registro actuales.

   ```
   tail -f /var/log/messages
   ```

   Se mostrarán varios mensajes en los que se identifica la unidad flash USB con un formato similar al del siguiente mensaje.

   ```
   Oct 25 13:25:23 ubuntu kernel: [ 712.447080] sd 3:0:0:0: [sdb] Attached SCSI removable
   disk
   ```

   En este ejemplo, `sdb` identifica el dispositivo USB. Si su dispositivo se identifica de un modo diferente, use esa identificación en lugar de *sdb*.

3 Sobrescriba toda la unidad USB con la imagen ISO. Esto sobrescribe la tabla de particiones y todo el contenido anterior existente en la unidad USB.

   ```
   dd bs=10M if=VMware-VMvisor-Installer-version_number-build_number.x86_64.iso
   of=/dev/sdb
   ```

4 Expulsar la unidad USB.

   ```
   eject /dev/sdb
   ```

Resultados

Puede utilizar la unidad flash USB para arrancar el instalador de ESXi.

Crear una unidad flash USB para almacenar el script de instalación o actualización de ESXi

Puede utilizar una unidad flash USB para almacenar el script de instalación o actualización de ESXi que se va a utilizar para la instalación o actualización por script de ESXi.

Si existen varias unidades flash USB en el equipo de instalación, el software de instalación busca el script de instalación o actualización en todas las unidades flash USB que estén conectadas.

En las instrucciones de este procedimiento se supone que la unidad flash USB se detecta como `/dev/sdb`.

Nota No almacene el archivo `ks` que contiene el script de instalación o actualización en la misma unidad flash USB que se utiliza para arrancar la instalación o la actualización.

Requisitos previos

- Equipo Linux

- Script de instalación o actualización de ESXi, el archivo kickstart `ks.cfg`
- Unidad flash USB

Procedimiento

1 Conecte la unidad flash USB a un equipo Linux con acceso al script de instalación o actualización.

2 Cree una tabla de particiones.

   `/sbin/fdisk /dev/sdb`

   a Escriba `d` para eliminar las particiones hasta que no quede ninguna.

   b Escriba `n` para crear la partición principal 1 que abarca todo el disco.

   c Escriba `t` para configurar el tipo para una configuración adecuada para el sistema de archivos FAT32, por ejemplo, **c**.

   d Escriba `p` para imprimir la tabla de particiones.

   El resultado debe ser similar al texto siguiente:

```
Disk /dev/sdb: 2004 MB, 2004877312 bytes
255 heads, 63 sectors/track, 243 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
   Device Boot      Start         End      Blocks   Id  System
/dev/sdb1             1           243      1951866  c   W95 FAT32 (LBA)
```

   e Escriba `w` para escribir la tabla de particiones y salir.

3 Formatee la unidad flash USB con el sistema de archivos FAT32.

   `/sbin/mkfs.vfat -F 32 -n USB /dev/sdb1`

4 Cree un directorio de destino y monte la unidad flash USB allí.

   `mkdir -p /usbdisk`

   `mount /dev/sdb1 /usbdisk`

5 Copie el script de instalación de ESXi en la unidad flash USB.

   `cp ks.cfg /usbdisk`

6 Desmonte la unidad flash USB.

   `umount /usbdisk`

Resultados

La unidad flash USB contiene el script de instalación o actualización de ESXi.

Pasos siguientes

Al arrancar el instalador de ESXi, apunte a la ubicación de la unidad flash USB del script de instalación o actualización. Consulte Introducir las opciones de arranque para ejecutar un script de instalación o actualización y Archivos de configuración PXELINUX.

Crear una imagen ISO de instalador con un script de instalación o actualización personalizado

Puede personalizar la imagen ISO del instalador de ESXi estándar con su propio script de instalación o actualización. Esta personalización permite realizar una instalación o actualización desatendida y generada por script cuando arranque la imagen ISO del instalador resultante.

Consulte también Instalar ESXi mediante un script y Acerca del archivo boot.cfg .

Requisitos previos

- Equipo Linux
- La imagen ISO de ESXi `VMware-VMvisor-Installer-`*`x.x.x-XXXXXX`*`.x86_64.iso`, donde *`x.x.x`* es la versión de ESXi que está instalando y *`XXXXXX`* es el número de compilación de la imagen ISO del instalador
- Su script de instalación o actualización personalizado, el archivo de inicio de actividad `KS_CUST.CFG`

Procedimiento

1 Descargue la imagen ISO de ESXi desde el portal de soporte de Broadcom.

2 Monte la imagen ISO en una carpeta:

   `mount -o loop VMware-VMvisor-Installer-x.x.x-XXXXXX.x86_64.iso /esxi_cdrom_mount`

   `XXXXXX` es el número de versión de ESXi para la versión que está instalado o la versión a la que está actualizando.

3 Copie el contenido de `esxi_cdrom` en otra carpeta:

   `cp -r /esxi_cdrom_mount/* /esxi_cdrom`

4 Copie el archivo de inicio a `/esxi_cdrom`.

   `cp KS_CUST.CFG /esxi_cdrom`

5 Modifique el archivo `boot.cfg` tanto en `/esxi_cdrom/efi/boot/boot.cfg` (para arranque UEFI) como en `/esxi_cdrom/boot.cfg` (para arranque de BIOS heredado) para especificar la ubicación del script de instalación o actualización mediante la opción `kernelopt`.

   Debe utilizar caracteres en mayúscula para proporcionar la ruta de acceso del script, por ejemplo,

   ```
   kernelopt=runweasel ks=cdrom:/KS_CUST.CFG
   ```

Este paso automatiza la instalación o la actualización, sin la necesidad de especificar el archivo de inicio durante este proceso.

6 Vuelva a crear la imagen ISO con el comando `mkisofs` o `genisoimage`.

Comando	Sintaxis
mkisofs	**mkisofs -relaxed-filenames -J -R -o custom_esxi.iso -b ISOLINUX.BIN -c BOOT.CAT -no-emul-boot -boot-load-size 4 -boot-info-table -eltorito-alt-boot -eltorito-platform efi -b EFIBOOT.IMG -no-emul-boot /esxi_cdrom**
genisoimage	**genisoimage -relaxed-filenames -J -R -o custom_esxi.iso -b ISOLINUX.BIN -c BOOT.CAT -no-emul-boot -boot-load-size 4 -boot-info-table -eltorito-alt-boot -e EFIBOOT.IMG -no-emul-boot /esxi_cdrom**

Esta imagen de instalador ISO se puede utilizar para un arranque normal o un arranque seguro UEFI. No obstante, vSphere Lifecycle Manager no puede comprobar la suma de comprobación de dicha imagen ISO y no puede utilizarse para las actualizaciones mediante flujos de trabajo de vSphere Lifecycle Manager.

Resultados

La imagen ISO incluye su script de instalación o actualización personalizado.

Pasos siguientes

Instale ESXi desde la imagen ISO.

Descarga del instalador de ESXi

El software del instalador de ESXi se puede obtener desde un OEM o desde el portal de soporte de Broadcom.

Regístrese en el portal de soporte de Broadcom. Para obtener más información, consulte Registrar una cuenta en las comunidades y en el portal de soporte de Broadcom.

Para ver instrucciones de descarga de productos, consulte Descargar productos y software de Broadcom.

Para descargar archivos ZIP de paquetes sin conexión para actualizaciones y revisiones de ESXi, consulte Descargar archivos y soluciones PTF de Broadcom.

Para obtener más información, consulte Preguntas frecuentes de VMware al soporte de Broadcom.

Identificadores y nombres de dispositivos de almacenamiento de ESXi

En el entorno de ESXi, cada dispositivo de almacenamiento se identifica con varios nombres.

Identificadores de dispositivo

Según el tipo de almacenamiento, el host ESXi utiliza distintos algoritmos y convenciones para generar un identificador para cada dispositivo de almacenamiento.

Identificadores provistos por el almacenamiento

El host ESXi consulta a un dispositivo de almacenamiento de destino el nombre del dispositivo. A partir de los metadatos devueltos, el host extrae o genera un identificador único para el dispositivo. El identificador se basa en estándares de almacenamiento específico, es persistente y único en todos los hosts; además, tiene uno de los formatos siguientes:

- naa.*xxx*
- eui.*xxx*
- t10.*xxx*

Identificador basado en rutas

Cuando el dispositivo no proporciona un identificador, el host genera un nombre mpx.*path*, donde *path* representa la primera ruta de acceso al dispositivo, por ejemplo, `mpx.vmhba1:C0:T1:L3`. Este identificador puede usarse de la misma forma que el identificador proporcionado por el almacenamiento.

El identificador mpx.*ruta* se crea para dispositivos locales asumiendo que los nombres de ruta son únicos. Sin embargo, este identificador no es único ni persistente y puede cambiar después de reiniciar todos los sistemas.

Generalmente, la ruta de acceso al dispositivo tiene el formato siguiente:

vmhba*Adapter*:C*Channel*:T*Target*:L*LUN*

- vmhba*Adapter* es el nombre del adaptador de almacenamiento. El nombre se refiere al adaptador físico en el host, no a la controladora SCSI que usan las máquinas virtuales.
- C*Channel* es el número de canal de almacenamiento.

  Los adaptadores de iSCSI de software y los adaptadores de hardware dependiente utilizan el número de canal para mostrar varias rutas de acceso al mismo destino.
- T*Target* es el número de destino. El host determina la numeración de destinos y esta puede cambiar cuando las asignaciones de destinos visibles para el host cambian. Los destinos compartidos entre distintos hosts no pueden tener el mismo número de destino.
- L*LUN* es el número LUN que muestra la posición del LUN en el destino. El número LUN se obtiene del sistema de almacenamiento. Si un destino tiene un solo LUN, el número LUN siempre es cero (0).

Por ejemplo, `vmhba1:C0:T3:L1` representa al LUN1 en el destino 3 al que se accede a través del adaptador de almacenamiento vmhba1 y del canal 0.

Identificador heredado

Además del identificador proporcionado por el dispositivo o mpx.*ruta*, ESXi genera un nombre heredado alternativo para cada dispositivo. El identificador tiene el formato siguiente:

vml.*number*

El identificador heredado incluye una serie de dígitos que son únicos para el dispositivo. El identificador puede proceder en parte de los metadatos que se obtienen a través del comando SCSI INQUIRY. En los dispositivos no locales que no proporcionan identificadores SCSI INQUIRY, el identificador vml.*number* se utiliza como el único identificador exclusivo disponible.

Ejemplo: Mostrar nombres de dispositivo en vSphere CLI

Puede utilizar el comando `esxcli storage core device list` para mostrar todos los nombres de dispositivo en la CLI de vSphere. El resultado es similar al ejemplo siguiente:

```
# esxcli storage core device list
naa.XXX
      Display Name: DGC Fibre Channel Disk(naa.XXX)
      ...
      Other UIDs: vml.000XXX
mpx.vmhba1:C0:T0:L0
   Display Name: Local VMware Disk (mpx.vmhba1:C0:T0:L0)
   ...
   Other UIDs: vml.0000000000XYZ
```

Actualizar hosts de forma interactiva

Para actualizar hosts ESXi 6.7 o ESXi 7.0 a ESXi 8.0, puede arrancar el instalador de ESXi desde un CD, un DVD o una unidad flash USB.

Antes de realizar la actualización, considere la posibilidad de desconectar el almacenamiento de red. Esta acción disminuye el tiempo que tarda el instalador en buscar unidades de disco disponibles. Al desconectar el almacenamiento de red, ninguno de los archivos almacenados en los discos desconectados está disponible durante la instalación. No desconecte un LUN que contenga una instalación existente de ESXi.

Nota No se admite la actualización interactiva en hosts ESXi con una unidad de procesamiento de datos (DPU).

Requisitos previos

- Compruebe que la imagen ISO del instalador de ESXi esté en una de las ubicaciones siguientes:
  - Un CD o DVD. Si no tiene el CD o DVD de instalación, puede crear uno. Consulte Descargar y grabar un CD or DVD de la imagen ISO del instalador de ESXi

- Una unidad flash USB. Consulte Formatear una unidad flash USB para arrancar la instalación o la actualización de ESXi

Nota También puede usar PXE para arrancar el instalador de ESXi y ejecutar una instalación interactiva o una instalación generada por script. Consulte Descripción general de la instalación para el arranque de red.

- Compruebe que el reloj de hardware del servidor esté configurado como UTC. Este ajuste se encuentra en el BIOS o la UEFI del sistema.
- ESXi Embedded no debe estar en el host. ESXi Installable y ESXi Embedded no pueden coexistir en el mismo host.
- Si va a actualizar un host ESXi, se migrarán los VIB personalizados compatibles que no se incluyen en la imagen ISO del instalador de ESXi. Consulte Actualización de hosts con VIB personalizados de terceros
- Consulte la documentación del proveedor del hardware para obtener información sobre cómo cambiar el orden de arranque.

Procedimiento

1 Inserte el CD o DVD del instalador de ESXi en la unidad de CD-ROM/DVD-ROM o conecte la unidad flash USB del instalador y reinicie la máquina.

2 Configure el BIOS o la UEFI para que arranque desde el dispositivo de CD-ROM o la unidad flash USB.

3 En el panel Seleccionar un disco, seleccione la unidad en la que desea instalar o actualizar ESXi y presione Intro.

Presione F1 para obtener más información sobre el disco seleccionado.

Nota No se base en el orden de discos de la lista para seleccionar un disco. El BIOS o la UEFI determinan el orden de los discos. En los sistemas en los que continuamente se agregan o quitan unidades, es posible que estas unidades no estén ordenadas.

4 Actualice o instale ESXi si el instalador encuentra una instalación de ESXi y un almacén de datos de VMFS existentes.

Si no es posible conservar un almacén de datos existente de VMFS, únicamente puede optar por instalar ESXi y sobrescribir el almacén de datos existente de VMFS o cancelar la instalación. Si opta por sobrescribir el almacén de datos existente de VMFS, primero debe crear una copia de seguridad del almacén de datos.

5 Presione F11 para confirmar e iniciar la actualización.

6 Una vez finalizada la actualización, retire la unidad flash USB, o el CD o el DVD de instalación.

7 Presione Intro para reiniciar el host.

8 Como primer dispositivo de arranque, establezca la unidad que seleccionó previamente al actualizar ESXi.

Instalar o actualizar hosts mediante un script

Puede implementar hosts de ESXi rápidamente mediante instalaciones o actualizaciones desatendidas generadas por script.

Las instalaciones o las actualizaciones generadas por script proporcionan un mecanismo eficaz para la implementación de varios hosts. El script de instalación o actualización contiene la configuración de instalación para ESXi. Puede aplicar el script a todos los que desee que tengan una configuración similar.

Para una instalación o una actualización generada por script, debe usar los comandos compatibles para crear un script. Puede editar el script con la finalidad de cambiar ajustes de configuración que sean exclusivos para cada host.

El script de instalación o actualización puede residir en una de las ubicaciones siguientes:

- Servidor FTP
- Servidor HTTP/HTTPS
- servidor NFS
- Unidad flash USB
- Unidad de CD-ROM

Introducir las opciones de arranque para ejecutar un script de instalación o actualización

Puede iniciar un script de instalación o actualización introduciendo las opciones de arranque en la línea de comandos de arranque del instalador de ESXi.

En el momento del arranque, es posible que necesite especificar opciones para acceder al archivo de inicio. Puede introducir opciones de arranque presionando Shift+O en el gestor de arranque. Para una instalación de arranque PXE, puede pasar opciones a través de la línea `kernelopts` del archivo `boot.cfg`. Consulte Acerca del archivo boot.cfg y Arranque de red del instalador de ESXi.

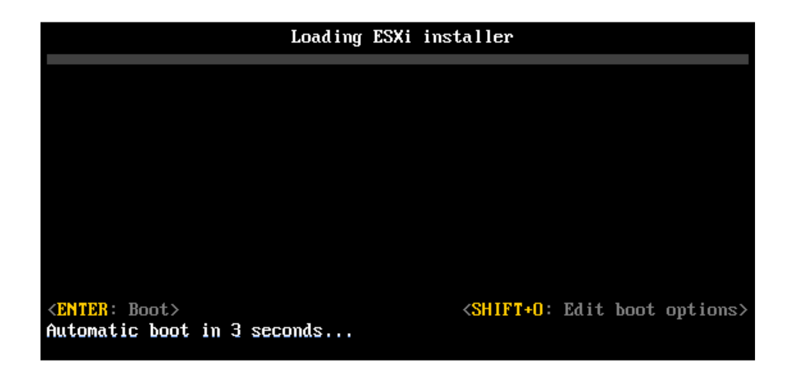
Para especificar la ubicación del script de instalación, defina la opción `ks=`*`filepath`*, donde *filepath* indica la ubicación del archivo Kickstart. De lo contrario, no se podrá iniciar una instalación o actualización generadas por script. Si se omite `ks=`*`filepath`*, se ejecuta el instalador de texto.

Las opciones de arranque compatibles se detallan en Opciones de arranque .

Procedimiento

1 Inicie el host.

2 Cuando aparezca la ventana del instalador de ESXi, presione las teclas Mayús + O para editar las opciones de arranque.



3 En el símbolo del sistema `runweasel`, introduzca **`ks=`*`ubicación del script de instalación más las opciones de la línea de comandos de arranque`***.

Ejemplo: Opción de arranque

Introduzca las siguientes opciones de arranque:

```
ks=http://00.00.00.00/kickstart/ks-osdc-pdp101.cfg nameserver=00.00.0.0 ip=00.00.00.000
netmask=255.255.255.0 gateway=00.00.00.000
```

Opciones de arranque

Cuando realice una instalación por script, es posible que necesite especificar opciones en el arranque para acceder al archivo de inicio.

Opciones de arranque compatibles

Tabla 3-7. Opciones de arranque para la instalación de ESXi

Opción de arranque	Descripción
`BOOTIF=`*`hwtype-MAC address`*	Similar a la opción `netdevice`, excepto en el formato PXELINUX, tal como se describe en la opción IPAPPEND en SYSLINUX en el sitio `syslinux.org`.
`gateway=`*`ip address`*	Permite establecer esta puerta de enlace de red como la puerta de enlace predeterminada para utilizarla en la descarga de scripts de instalación y medios de instalación.
`ip=`*`ip address`*	Permite configurar una dirección IP estática para utilizarla en la descarga de scripts de instalación y medios de instalación. Nota: también se admite el formato PXELINUX para esta opción. Consulte la opción IPAPPEND en SYSLINUX en el sitio `syslinux.org`.

Tabla 3-7. Opciones de arranque para la instalación de ESXi (continuación)

Opción de arranque	Descripción
ks=cdrom:/*path*	Permite realizar una instalación por script con el script en *path*, que se encuentra en el CD de la unidad de CD-ROM. Cada CDROM se monta y se comprueba hasta que se encuentre el archivo que coincida con la ruta de acceso. **Importante** Si creó una imagen ISO de instalador con un script de instalación o actualización personalizado, debe utilizar caracteres en mayúscula para proporcionar la ruta de acceso del script, por ejemplo, ks=cdrom:/KS_CUST.CFG.
ks=file://*path*	Realiza una instalación por script con el script en *path*.
ks=*protocol*://*serverpath*	Realiza una instalación por script con un script ubicado en la red en la dirección URL determinada. El *protocolo* puede ser http, https, ftp o nfs. Un ejemplo de uso del protocolo NFS es ks=nfs://*host*/*porturl-path*. El formato de la URL de NFS se especifica en RFC 2224.
ks=usb	Realiza una instalación por script mediante el acceso al script desde la unidad USB conectada. Busca un archivo con el nombre ks.cfg. El archivo debe estar ubicado en el directorio raíz de la unidad. Si se conectan varias unidades flash USB, se realizará la búsqueda hasta que se encuentre el archivo ks.cfg. Solo se admiten los sistemas de archivos FAT16 y FAT32.
ks=usb:/*path*	Realiza una instalación por script con un archivo de script en la ruta especificada, que se encuentra en USB.
ksdevice=*device*	Intenta utilizar un adaptador de red *device* cuando se realiza la búsqueda de un script de instalación y un medio de instalación. Se especifica como una dirección MAC, por ejemplo, 00:50:56:C0:00:01. Esta ubicación también puede ser un nombre vmnicNN. Si no se especifica y los archivos deben obtenerse a través de la red, el instalador utiliza de forma predeterminada el primer adaptador de red detectado que esté conectado.
nameserver=*ip address*	Especifica un servidor de nombres de dominio para utilizarlo en la descarga de scripts de instalación y medios de instalación.
netdevice=*device*	Intenta utilizar un adaptador de red *device* cuando se realiza la búsqueda de un script de instalación y un medio de instalación. Se especifica como una dirección MAC, por ejemplo, 00:50:56:C0:00:01. Esta ubicación también puede ser un nombre vmnicNN. Si no se especifica y los archivos deben obtenerse a través de la red, el instalador utiliza de forma predeterminada el primer adaptador de red detectado que esté conectado.
netmask=*subnet mask*	Especifica una máscara de subred para la interfaz de red que descarga los scripts de instalación y los medios de instalación.

Tabla 3-7. Opciones de arranque para la instalación de ESXi (continuación)

Opción de arranque	Descripción
`vlanid=`*`vlanid`*	Configure la tarjeta de red para que se encuentre en la VLAN especificada.
`systemMediaSize=`*`small`*	Limita el tamaño de las particiones de almacenamiento del sistema en los medios de arranque. El valor seleccionado debe adecuarse al propósito del sistema. Se puede elegir alguno de los siguientes valores: ■ *min* (32 GB, para servidores integrados o con un único disco) ■ *small* (64 GB, para servidores con al menos 512 GB de RAM) ■ *default* (128 GB) ■ *max* (consumir todo el espacio disponible, para servidores de varios terabytes)

Para más información sobre las opciones de inicio de ESXi posteriores a la instalación, consulte el artículo 77009 de la base de conocimientos de VMware.

Instalar ESXi mediante un script

El script de instalación o actualización es un archivo de texto que contiene los comandos compatibles (por ejemplo, `ks.cfg`).

La sección de comandos del script contiene las opciones de instalación de ESXi. Esta sección es obligatoria y debe aparecer primero en el script.

Acerca del archivo boot.cfg

El archivo de configuración del cargador de arranque `boot.cfg` especifica el kernel, las opciones del kernel y los módulos de arranque que utiliza el cargador de arranque `mboot.c32` o `mboot.efi` en una instalación de ESXi.

El archivo `boot.cfg` se incluye en el instalador de ESXi. Puede modificar la línea `kernelopt` del archivo `boot.cfg` para especificar la ubicación de un script de instalación o para pasar otras opciones de arranque.

El archivo `boot.cfg` tiene la siguiente sintaxis:

```
# boot.cfg -- mboot configuration file
#
# Any line preceded with '#' is a comment.

title=STRING
prefix=DIRPATH
kernel=FILEPATH
kernelopt=STRING
modules=FILEPATH1 --- FILEPATH2... --- FILEPATHn

# Any other line must remain unchanged.
```

Los comandos de `boot.cfg` configuran el cargador de arranque.

Tabla 3-8. Comandos de `boot.cfg`.

Comando	Descripción
`title=`*`STRING`*	Establece el título del cargador de arranque como *`STRING`*.
`prefix=`*`STRING`*	(Opcional) Agrega *`DIRPATH/`* frente a cada *`FILEPATH`* en los comandos `kernel=` y `modules=` que no empiezan con / o con `http://`.
`kernel=`*`FILEPATH`*	Establece la ruta de acceso del kernel como *`FILEPATH`*.
`kernelopt=`*`STRING`*	Anexa *`STRING`* a las opciones de arranque del kernel.
`modules=`*`FILEPATH1`* `---` *`FILEPATH2...`* `---` *`FILEPATHn`*	Enumera los módulos que se van a cargar, separados por tres guiones (`---`).

Consulte Crear una imagen ISO de instalador con un script de instalación o actualización personalizado y Arranque de red del instalador de ESXi.

Ubicaciones admitidas para scripts de instalación o actualización

En instalaciones y actualizaciones generadas por script, el instalador de ESXi puede acceder al script de la instalación o actualización, que también se conoce como el archivo inicial, desde varias ubicaciones.

Se admiten las siguientes ubicaciones para el script de instalación o actualización:

- CD/DVD. Consulte Crear una imagen ISO de instalador con un script de instalación o actualización personalizado.
- Unidad flash USB. Consulte Crear una unidad flash USB para almacenar el script de instalación o actualización de ESXi.
- Una ubicación local de red a la que se puede acceder mediante los siguientes protocolos: NFS, HTTP, HTTPS, FTP

Ruta de acceso del script de instalación o actualización

Puede especificar la ruta de acceso de un script de instalación o actualización.

`ks=http://`*`XXX.XXX.XXX.XXX`*`/kickstart/KS.CFG` es la ruta de acceso del script de instalación de ESXi, donde*`XXX.XXX.XXX.XXX`*es la dirección IP del equipo donde reside el script. Consulte Instalar ESXi mediante un script.

Para iniciar un script de instalación desde una instalación interactiva, escriba la opción `ks=` de forma manual. Consulte Introducir las opciones de arranque para ejecutar un script de instalación o actualización.

Comandos de scripts de instalación y actualización

Para modificar el script predeterminado de instalación o actualización, o para crear su propio script, use comandos compatibles. Use comandos compatibles en el script de instalación, que se especifica mediante un comando de arranque cuando se arranca el instalador.

Para determinar en qué disco instalar o actualizar ESXi, el script de instalación requiere uno de los comandos siguientes: `install`, `upgrade` o `installorupgrade`. El comando `install` crea las particiones predeterminadas, que incluyen un almacén de datos de VMFS que ocupa todo el espacio disponible después de que se crean las demás particiones.

Con vSphere 8.0, si el sistema tiene unidades de procesamiento de datos (DPU) admitidas, considere siempre la posibilidad de instalación, reinstalación o actualización de ESXi en las DPU además de ESXi en los hosts. La actualización de ESXi y la actualización en las DPU no es compatible con el método interactivo o con scripts, solo se puede usar vSphere Lifecycle Manager.

Nota El uso de dispositivos SD y USB para almacenar particiones de ESX-OSData está cayendo es desuso. Puede usar dispositivos SD y USB solo para crear particiones de banco de arranque, `boot-bank 0` y `boot-bank 1`. También puede proporcionar un disco persistente de 32 GB como mínimo para instalar la partición ESX-OSData. Para definir estos discos, utilice el parámetro `systemDisk` en el comando `install`.

---

accepteula o vmaccepteula (obligatorio)

Acepta el contrato de licencia de ESXi.

clearpart (opcional)

Borra las particiones existentes del disco. Requiere que se especifique el comando `install`. Edite cuidadosamente el comando `clearpart` en sus scripts existentes.

--drives=	Quita las particiones en las unidades especificadas.
--alldrives	Ignora el requisito de `--drives=` y permite borrar las particiones de cada unidad.
--ignoredrives=	Elimina las particiones en todas las unidades, excepto las especificadas. Es obligatorio a menos que se especifiquen las marcas `--drives=` o `--alldrives`.

`--overwritevmfs`

Permite sobrescribir las particiones de VMFS en las unidades especificadas. De forma predeterminada, no se permite sobrescribir las particiones de VMFS.

`--firstdisk=`

`tipo-disco1`

`[`*`tipo-disco2`*`,...]`

Nota Si la versión del sistema vSphere es anterior a la 8.0 Update 3 y tiene DPU, también debe especificar una ranura PCI: `install --firstdisk --overwritevmfs --dpupcislots=<PCIeSlotID>`. Para los sistemas con la versión 8.0 Update 3 y posteriores, el parámetro `dpupcislots` ha quedado obsoleto.

Particiona el primer disco encontrado que satisface las condiciones. De forma predeterminada, los discos que satisfacen las condiciones se ordenan en el orden siguiente:

1 Almacenamiento conectado a nivel local (`local`)

2 Almacenamiento en red (`remote`)

Puede cambiar el orden de los discos anexando una lista separada por comas al argumento. Si proporciona una lista de filtros, se sobrescribe la configuración predeterminada. Puede combinar filtros para especificar un disco en particular, lo que incluye `esx` para el primer disco en el que se haya instalado ESXi, la información de modelo y proveedor, o el nombre del controlador del dispositivo VMkernel. Por ejemplo, para dar preferencia a un disco con el nombre de modelo ST3120814A y a cualquier disco que use el controlador mptsas en lugar de un disco local normal, el argumento es `--firstdisk=ST3120814A,mptsas,local`. Puede utilizar `localesx` para el almacenamiento local que contiene la imagen de ESXi o `remoteesx` para el almacenamiento remoto que contiene la imagen deESXi.

dryrun (opcional)

Analiza y comprueba el script de instalación. No ejecuta la instalación.

instalar

Especifica que se trata de una instalación nueva. Se requieren los comandos `install`, `upgrade` o `installorupgrade` para determinar en qué disco se debe instalar o actualizar ESXi.

`--disk= or --drive=`

Especifica el disco que se particionará. En el comando `--disk=`*`diskname`*, *diskname* puede ser un nombre de disco o una ruta completa de sistema de archivos de disco en ESXi, por ejemplo:

- Nombre de disco: `--disk=naa.6d09466044143600247aee55ca2a6405` o

- Ruta de acceso del dispositivo: --disk=*/vmfs/devices/disks/mpx.vmhba1:C0:T0:L0*

Para conocer los formatos admitidos de nombre de disco, consulte Nombre de los dispositivos de disco.

--firstdisk=*tipo-disco1*, [*tipo-disco2*,...]

Nota Si la versión del sistema vSphere es anterior a la 8.0 Update 3 y tiene DPU, también debe especificar una ranura PCI: install --firstdisk --overwritevmfs --dpupcislots=<PCIeSlotID>. Para los sistemas con la versión 8.0 Update 3 y posteriores, el parámetro dpupcislots ha quedado obsoleto.

Particiona el primer disco encontrado que satisface las condiciones. De forma predeterminada, los discos que satisfacen las condiciones se ordenan en el orden siguiente:

1 Almacenamiento conectado a nivel local (local)

2 Almacenamiento en red (remote)

Puede cambiar el orden de los discos anexando una lista separada por comas al argumento. Si proporciona una lista de filtros, se sobrescribe la configuración predeterminada. Puede combinar filtros para especificar un disco en particular, lo que incluye esx para el primer disco en el que se haya instalado ESX, la información de modelo y proveedor, o el nombre del controlador del dispositivo VMkernel. Por ejemplo, para dar preferencia a un disco con el nombre de modelo ST3120814A y a cualquier disco que use el controlador mptsas en lugar de un disco local normal, el argumento es --firstdisk=ST3120814A,mptsas,local. Puede utilizar localesx para el almacenamiento local que contiene la imagen de ESXi o remoteesx para el almacenamiento remoto que contiene la imagen deESXi.

--ignoressd

Excluye los discos de estado sólido de los que satisfacen las condiciones para el particionamiento. Esta opción puede utilizarse con el comando install y la opción --firstdisk. Esta opción tiene prioridad sobre la opción --firstdisk. Esta opción no es válida con las opciones --drive o --disk ni con los comandos upgrade o installorupgrade. Consulte la documentación de *Almacenamiento de vSphere* para obtener más información sobre la prevención del formateo de SSD durante la creación automática de particiones.

--overwritevsan

Debe usar la opción --overwritevsan cuando instale ESXi en un disco, ya sea SSD o HDD (magnética), que forme parte de un grupo de discos de vSAN. Si usa esta opción y no hay ninguna partición de

vSAN en el disco seleccionado, se produce un error en la instalación. Al instalar ESXi en un disco que forma parte de un grupo de discos de vSAN, el resultado depende del disco que se selecciona:

- Si selecciona una SSD, esta y todas las HDD subyacentes del mismo grupo de discos se borrarán.
- Si selecciona una HDD y el tamaño del grupo de discos es mayor que 2, solo se borrará la HDD seleccionada.
- Si selecciona una HDD y el tamaño del grupo de discos es 2 o menos, se borrarán la SSD y la HDD seleccionada.

Para obtener más información acerca de la administración de grupos de discos de vSAN, consulte la documentación de *Almacenamiento de vSphere*.

--overwritevmfs

Es obligatorio para sobrescribir un almacén de datos existente de VMFS en el disco antes de la instalación.

--preservevmfs

Conserva el almacén de datos existente de VMFS en el disco durante la instalación.

--novmfsondisk

Impide que se cree una partición de VMFS en este disco. Debe utilizarse con `--overwritevmfs` si existe una partición de VMFS en el disco.

--systemdisk

Si utiliza un dispositivo USB o SD, `systemDisk` especifica el disco persistente local en el que se instalará la partición ESX-OSData. Por ejemplo, **install --firstdisk = usb --systemDisk=<diskID>**. Como resultado, las particiones de banco de arranque se colocan en el dispositivo USB, mientras que la partición de OSData se encuentra en el disco especificado en el parámetro `systemDisk`.

--repartitionsystemdisk

Si utiliza un dispositivo USB o SD y el disco local que especificó con el parámetro `systemDisk` no está vacío o contiene un almacén de datos, puede usar `repartitionSystemDisk` para asegurarse de que el disco persistente se vuelva a particionar antes de usarlo.

Nota Si un disco persistente local no está disponible o el tamaño del disco es inferior a 32 GB, verá mensajes de advertencia, pero la instalación continúa.

--forceunsupportedinstall

Bloquea la instalación de CPU obsoletas.

installorupgrade

Se requieren los comandos `install`, `upgrade` o `installorupgrade` para determinar en qué disco se debe instalar o actualizar ESXi.

`--disk= or --drive=`

Especifica el disco que se particionará. En el comando `--disk=`*`diskname`*, *diskname* puede ser un nombre de disco o una ruta completa de sistema de archivos de disco en ESXi, por ejemplo:

- Nombre de disco: `--disk=naa.6d09466044143600247aee55ca2a6405` o
- Ruta de acceso del dispositivo: `--disk=`*`/vmfs/devices/disks/mpx.vmhba1:C0:T0:L0`*

Para conocer los formatos admitidos de nombre de disco, consulte Nombre de los dispositivos de disco.

`--firstdisk=`

`tipo-disco1,`

`[`*`tipo-disco2`*`,...]`

Nota Si la versión del sistema vSphere es anterior a la 8.0 Update 3 y tiene DPU, también debe especificar una ranura PCI: `install --firstdisk --overwritevmfs --dpupcislots=<PCIeSlotID>`. Para los sistemas con la versión 8.0 Update 3 y posteriores, el parámetro `dpupcislots` ha quedado obsoleto.

Particiona el primer disco encontrado que satisface las condiciones. De forma predeterminada, los discos que satisfacen las condiciones se ordenan en el orden siguiente:

1 Almacenamiento conectado a nivel local (`local`)

2 Almacenamiento en red (`remote`)

Puede cambiar el orden de los discos anexando una lista separada por comas al argumento. Si proporciona una lista de filtros, se sobrescribe la configuración predeterminada. Puede combinar filtros para especificar un disco en particular, lo que incluye `esx` para el primer disco en el que se haya instalado ESX, la información de modelo y proveedor, o el nombre del controlador del dispositivo VMkernel. Por ejemplo, para dar preferencia a un disco con el nombre de modelo ST3120814A y a cualquier disco que use el controlador mptsas en lugar de un disco local normal, el argumento es `--firstdisk=ST3120814A,mptsas,local`. Puede utilizar `localesx` para el almacenamiento local que contiene la imagen de ESXi o `remoteesx` para el almacenamiento remoto que contiene la imagen deESXi.

`--overwritevsan`

Debe usar la opción `--overwritevsan` cuando instale ESXi en un disco, ya sea SSD o HDD (magnética), que forme parte de un grupo de discos de vSAN. Si usa esta opción y no hay ninguna partición de

	vSAN en el disco seleccionado, se produce un error en la instalación. Al instalar ESXi en un disco que forma parte de un grupo de discos de vSAN, el resultado depende del disco que se selecciona: ■ Si selecciona una SSD, esta y todas las HDD subyacentes del mismo grupo de discos se borrarán. ■ Si selecciona una HDD y el tamaño del grupo de discos es mayor que 2, solo se borrará la HDD seleccionada. ■ Si selecciona una HDD y el tamaño del grupo de discos es 2 o menos, se borrarán la SSD y la HDD seleccionada. Para obtener más información acerca de la administración de grupos de discos de vSAN, consulte la documentación de *Almacenamiento de vSphere*.
`--overwritevmfs`	Instale ESXi si en el disco existe una partición de VMFS, pero no una instalación de ESX ni ESXi. A menos que esta opción esté presente, se producirá un error en el instalador si en el disco existe una partición de VMFS, pero no una instalación de ESX o de ESXi.

keyboard (opcional)

Configura el tipo de teclado para el sistema.

`keyboardType`	Especifica el mapa del teclado para el tipo de teclado seleccionado. *keyboardType* debe ser uno de los siguientes tipos. ■ Belgian ■ Brazilian ■ Croatian ■ Czechoslovakian ■ Danish ■ Estonian ■ Finnish ■ Francés ■ Alemán ■ Greek ■ Icelandic ■ Italian ■ Japonés

- Latin American
- Norwegian
- Polish
- Portuguese
- Russian
- Slovenian
- Español
- Swedish
- Swiss French
- Swiss German
- Turkish
- Ukrainian
- United Kingdom
- Inglés americano (predeterminado)
- US Dvorak

serialnum o vmserialnum (opcional)

El comando se admite en ESXi 5.1 y versiones posteriores. Configura las licencias. Si no se incluye, ESXi se instala en modo de evaluación.

--esx=<license-key>	Especifica la clave de licencia de vSphere que se utilizará. El formato corresponde a cinco grupos de cinco caracteres (XXXXX-XXXXX-XXXXX-XXXXX-XXXXX).

network (opcional)

Especifica una dirección de red para el sistema.

--bootproto=[dhcp|static]	Especifica si la configuración de red se debe obtener desde DHCP o si se debe configurar de forma manual.
--device=	Especifica la dirección MAC de la tarjeta de red o el nombre del dispositivo, con el formato `vmnicNN` (por ejemplo, `vmnic0`). Esta opción hace referencia al dispositivo del vínculo superior para el conmutador virtual.
--ip=	Establece una dirección IP para el equipo que se va a instalar, con el formato `xxx.xxx.xxx.xxx`. Es obligatorio cuando se usa la opción `--bootproto=static` y se ignora en los demás casos.

`--gateway=`	Designa la puerta de enlace predeterminada como una dirección IP, con el formato `xxx.xxx.xxx.xxx`. Se usa con la opción `--bootproto=static`.
`--nameserver=`	Designa el servidor de nombre principal como una dirección IP. Se usa con la opción `--bootproto=static`. Omita esta opción si no va a usar DNS. La opción `--nameserver` puede admitir dos direcciones IP. Por ejemplo: `--nameserver="10.126.87.104[,10.126.87.120]"`
`--netmask=`	Especifica la máscara de subred para el sistema instalado, con el formato `255.xxx.xxx.xxx`. Se usa con la opción `--bootproto=static`.
`--hostname=`	Especifica el nombre de host para el sistema instalado.
`--vlanid=` ***`vlanid`***	Especifica la VLAN en la que reside el sistema. Se usa con las opciones `--bootproto=dhcp` o `--bootproto=static`. Se establece como un valor entero entre 1 y 4096.
`--addvmportgroup=(0|1)`	Especifica si se debe agregar el grupo de puertos de la red de máquinas virtuales (VM), que utilizan las máquinas virtuales. El valor predeterminado es 1.

paranoid (opcional)

Hace que los mensajes de advertencia interrumpan la instalación. Si omite este comando, los mensajes de advertencia se registran.

part o partition (opcional)

Crea un almacén de datos de VMFS en el sistema. Solo se puede crear un almacén de datos por cada disco. No se puede usar en el mismo disco que el comando `install`. Solo se puede especificar una partición por cada disco y solo puede ser una partición de VMFS.

`datastore name`	Especifica dónde se debe montar la partición.
`--ondisk= or --ondrive=`	Especifica el disco o la unidad en la que se crea la partición.
`--onfirstdisk=` ***`tipo-disco1,`*** **`[`*`tipo-disco2`*`,...]`**	**Nota** Si la versión del sistema vSphere es anterior a la 8.0 Update 3 y tiene DPU, también debe especificar una ranura PCI: `install --firstdisk --overwritevmfs --dpupcislots=<PCIeSlotID>`. Para los sistemas con la versión 8.0 Update 3 y posteriores, el parámetro `dpupcislots` ha quedado obsoleto.

Particiona el primer disco encontrado que satisface las condiciones. De forma predeterminada, los discos que satisfacen las condiciones se ordenan en el orden siguiente:

1 Almacenamiento conectado a nivel local (`local`)

2 Almacenamiento en red (`remote`)

Puede cambiar el orden de los discos anexando una lista separada por comas al argumento. Si proporciona una lista de filtros, se sobrescribe la configuración predeterminada. Puede combinar filtros para especificar un disco en particular, lo que incluye `esx` para el primer disco en el que se haya instalado ESX, la información de modelo y proveedor, o el nombre del controlador del dispositivo VMkernel. Por ejemplo, para dar preferencia a un disco con el nombre de modelo ST3120814A y a cualquier disco que use el controlador mptsas en lugar de un disco local normal, el argumento es `--onfirstdisk=ST3120814A,mptsas,local`. Puede utilizar `localesx` para el almacenamiento local que contiene la imagen de ESXi o `remoteesx` para el almacenamiento remoto que contiene la imagen deESXi.

reboot (opcional)

Reinicia la máquina después de que finaliza la instalación generada por script.

`<--noeject>`	No se expulsa el CD después de la instalación.

rootpw (obligatorio)

Configura la contraseña raíz para el sistema.

`--iscrypted`	Especifica que la contraseña está cifrada.
password	Especifica el valor de la contraseña.

actualizar

Se requieren los comandos `install`, `upgrade` o `installorupgrade` para determinar en qué disco se debe instalar o actualizar ESXi.

`--disk= or --drive=`

Especifica el disco que se particionará. En el comando `--disk=`*`diskname`*, *diskname* puede ser un nombre de disco o una ruta completa de sistema de archivos de disco en ESXi, por ejemplo:

- Nombre de disco: `--disk=naa.6d09466044143600247aee55ca2a6405` o
- Ruta de acceso del dispositivo: `--disk=`*`/vmfs/devices/disks/mpx.vmhba1:C0:T0:L0`*

	Para conocer los formatos admitidos de nombre de disco, consulte Nombre de los dispositivos de disco.
--firstdisk= ***tipo-disco1,*** **[*tipo-disco2*,...]**	Particiona el primer disco encontrado que satisface las condiciones. De forma predeterminada, los discos que satisfacen las condiciones se ordenan en el orden siguiente: 1 Almacenamiento conectado a nivel local (`local`) 2 Almacenamiento en red (`remote`) Puede cambiar el orden de los discos anexando una lista separada por comas al argumento. Si proporciona una lista de filtros, se sobrescribe la configuración predeterminada. Puede combinar filtros para especificar un disco en particular, lo que incluye `esx` para el primer disco en el que se haya instalado ESX, la información de modelo y proveedor, o el nombre del controlador del dispositivo VMkernel. Por ejemplo, para dar preferencia a un disco con el nombre de modelo ST3120814A y a cualquier disco que use el controlador mptsas en lugar de un disco local normal, el argumento es `--firstdisk=ST3120814A,mptsas,local`. Puede utilizar `localesx` para el almacenamiento local que contiene la imagen de ESXi o `remoteesx` para el almacenamiento remoto que contiene la imagen deESXi.

%include o include (opcional)

Especifica otro script de instalación para analizar. Este comando se utiliza de manera similar a un comando de varias líneas, pero usa solamente un argumento.

filename	Por ejemplo: `%include part.cfg`

%pre (opcional)

Especifica un script para ejecutar antes de que se evalúe la configuración de inicio. Por ejemplo, puede usarse para generar los archivos que incluirá el archivo de inicio.

--interpreter =[python|busybox]	Especifica el intérprete que se usará. El valor predeterminado es busybox.

%post (opcional)

Ejecuta el script especificado después de que finaliza la instalación del paquete. Si se especifican varias secciones `%post`, se ejecutan en el orden en que aparecen en el script de instalación.

--interpreter	Especifica el intérprete que se usará. El valor predeterminado es busybox.

=[python|busybox]	
--timeout=secs	Especifica el límite de tiempo de espera para la ejecución del script. Si el script no finalizó cuando se agota el tiempo de espera, el script se interrumpe de manera forzosa.
--ignorefailure =[true|false]	Si se configura como true, la instalación se considera correcta incluso si el script `%post` finalizó con un error.

%firstboot

Crea un script `init` que se ejecuta solamente durante el primer arranque. El script no afecta los arranques posteriores. Si se especifican varias secciones `%firstboot`, se ejecutan en el orden en que aparecen en el archivo de inicio.

Nota No es posible comprobar la semántica de los scripts `%firstboot` hasta el primer arranque del sistema. Un script `%firstboot` puede contener errores potencialmente catastróficos que no se detectan sino hasta después de la finalización de la instalación.

Importante El script `%firstboot` no se ejecuta si el arranque seguro está habilitado en el host ESXi.

--interpreter =[python|busybox]	Especifica el intérprete que se usará. El valor predeterminado es busybox.

Nota No es posible comprobar la semántica del script `%firstboot` hasta el primer arranque del sistema. Si el script contiene errores, no se detectan sino hasta después de la finalización de la instalación.

Instalar o actualizar ESXi desde un CD o DVD con un script

Puede instalar o actualizar ESXi desde una unidad de CD-ROM o DVD-ROM utilizando un script que especifique las opciones de instalación o actualización.

Puede iniciar el script de instalación o actualización introduciendo una opción de arranque cuando inicie el host. También puede crear una imagen ISO de instalador que incluya el script de instalación. Puede utilizar una imagen ISO de instalador para realizar una instalación generada por script y desatendida cuando arranque con la imagen ISO de instalador resultante. Consulte Crear una imagen ISO de instalador con un script de instalación o actualización personalizado.

Requisitos previos

Antes de ejecutar la instalación o la actualización generadas por script, asegúrese de que se cumplen los siguientes requisitos previos:

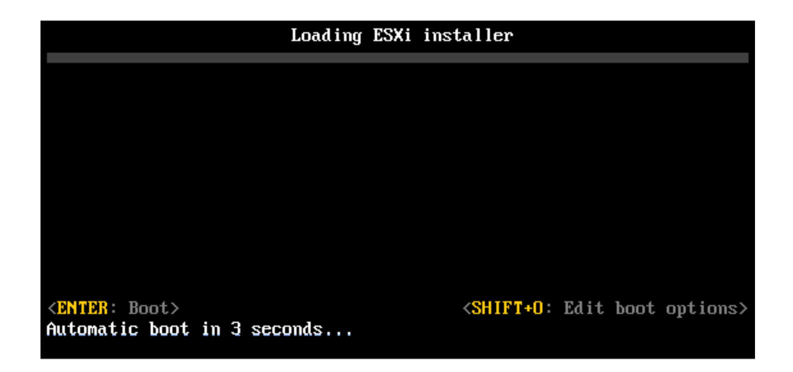
- El sistema en el que va a realizar la instalación o actualización cumple con los requisitos de hardware. Consulte Requisitos de hardware de ESXi.

- Tiene el ISO con el instalador de ESXi en un CD o DVD de instalación. Consulte Descargar y grabar un CD or DVD de la imagen ISO del instalador de ESXi.
- El sistema puede acceder al script de instalación o actualización predeterminado (`ks.cfg`) o a un script de instalación o actualización personalizado. Consulte Instalar ESXi mediante un script.
- Ha seleccionado un comando de arranque para ejecutar la instalación o actualización generada por script. Consulte Introducir las opciones de arranque para ejecutar un script de instalación o actualización. Para obtener una lista completa de los comandos de arranque, consulte Opciones de arranque .

Procedimiento

1 Arranque el instalador de ESXi desde la unidad de CD-ROM o DVD-ROM local.

2 Cuando aparezca la ventana del instalador de ESXi, presione las teclas Mayús + O para editar las opciones de arranque.



3 Introduzca una opción de arranque que invoque al archivo de script de instalación o actualización predeterminado o uno que haya creado.

   La opción de arranque tiene el formato `ks=`.

4 Presione Intro.

Resultados

Se ejecuta la operación de instalación, actualización o migración, utilizando las opciones que especificó.

Instalar o actualizar ESXi desde una unidad USB con un script

Puede instalar o actualizar ESXi desde una unidad flash USB utilizando un script que especifique las opciones de instalación o actualización.

Las opciones de arranque compatibles se detallan en Opciones de arranque .

Requisitos previos

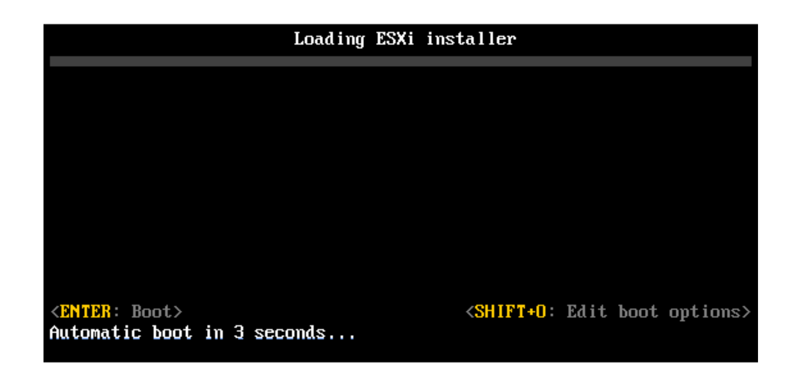
Antes de ejecutar la instalación o la actualización generadas por script, asegúrese de que se cumplen los siguientes requisitos previos:

- El sistema en el que va a realizar la instalación o la actualización a ESXi cumple con los requisitos de hardware para la instalación o la actualización. Consulte Requisitos de hardware de ESXi.
- Tiene el ISO con el instalador de ESXi en una unidad USB flash de arranque. Consulte Formatear una unidad flash USB para arrancar la instalación o la actualización de ESXi.
- El sistema puede acceder al script de instalación o actualización predeterminado (`ks.cfg`) o a un script de instalación o actualización personalizado. Consulte Instalar ESXi mediante un script.
- Ha seleccionado una opción de arranque para ejecutar la instalación, la actualización o la migración generadas por script. Consulte Introducir las opciones de arranque para ejecutar un script de instalación o actualización.

Procedimiento

1 Arranque el instalador de ESXi desde la unidad flash USB.

2 Cuando aparezca la ventana del instalador de ESXi, presione las teclas Mayús + O para editar las opciones de arranque.



3 Introduzca una opción de arranque que invoque al archivo de script de instalación o actualización predeterminado o uno que haya creado.

La opción de arranque tiene el formato `ks=`.

4 Presione Intro.

Resultados

Se ejecuta la operación de instalación, actualización o migración, utilizando las opciones que especificó.

Arranque de red del instalador ESXi para una instalación o actualización generadas por script

ESXi 8.0 ofrece varias opciones para utilizar para arrancar el instalador en una red y utilizar un script de instalación o actualización.

- Para obtener información sobre la configuración de una infraestructura de red, consulte Arranque de red del instalador de ESXi.
- Para obtener información sobre la creación y ubicación de un script de instalación, consulte Instalar ESXi mediante un script.
- Para conocer procedimientos específicos para utilizar el arranque de red para arrancar el instalador de ESXi y utilizar un script de instalación, consulte uno de los siguientes temas:
  - Arrancar el instalador de ESXi mediante HTTP de UEFI nativo
  - Arrancar el instalador de ESXi mediante iPXE y HTTP
  - Arrancar el instalador de ESXi mediante PXE y TFTP
- Para obtener información sobre la utilización de vSphere Auto Deploy para realizar una actualización generada por script a través de PXE para arrancar, consulte Capítulo 4 Usar vSphere Auto Deploy para reaprovisionar hosts .

Nombre de los dispositivos de disco

Para los comandos del script de instalación `install`, `upgrade` e `installorupgrade`, es necesario usar los nombres de dispositivos de disco.

Tabla 3-9. Nombre de los dispositivos de disco

Formato	Ejemplo	Descripción
NAA	naa.6d09466044143600247aee55ca2a6405	Identificador SCSI INQUIRY
EUI	eui.3966623838646463	Identificador SCSI INQUIRY
T10	t10.SanDisk00Cruzer_Blade000000004C5300 01171118101244	Identificador SCSI INQUIRY
VML	vml.00025261	Identificador de VMkernel heredado
MPX	mpx.vmhba0:C0:T0:L0	Identificador basado en rutas

Para obtener más información sobre los nombres de dispositivos de almacenamiento, consulte *Identificadores y nombres de dispositivos de almacenamiento* en la documentación de *Almacenamiento de vSphere*.

Cómo arrancar un host ESXi desde un dispositivo de red

Arranque de red del instalador de ESXi

Puede utilizar el entorno de ejecución previo al arranque (PXE) para arrancar un host ESXi desde un dispositivo de red si el host utiliza el UEFI o BIOS heredado.

De forma alternativa, si el host ESXi es compatible con UEFI HTTP nativo, puede utilizar el protocolo de transferencia de hipertexto (HTTP) para arrancar el host desde un dispositivo de red. ESXi se distribuye en un formato ISO que se utiliza para instalarse en la memoria flash o en un disco duro local. Puede extraer los archivos y arrancarlos a través de una interfaz de red.

PXE utiliza el protocolo de configuración dinámica de host (DHCP) y el protocolo trivial de transferencia de archivos (TFTP) para arrancar un sistema operativo a través de una red.

El arranque con PXE requiere determinada infraestructura de red y una máquina con un adaptador de red compatible con PXE. La mayoría de las máquinas que pueden ejecutar ESXi poseen adaptadores de red que pueden arrancar con PXE.

El UEFI HTTP nativo utiliza DHCP y HTTP para arrancar a través de una red. El arranque UEFI HTTP requiere una infraestructura de red, una versión de firmware UEFI en el host de ESXi que incluye la función de arranque HTTP y un adaptador de red que admita redes UEFI.

El arranque mediante HTTP es más rápido y fiable que el uso de TFTP. Esto se debe a las capacidades del protocolo TCP subyacente a HTTP, como la transmisión integrada y la recuperación de paquetes perdidos. Si los hosts ESXi no son compatibles con el protocolo UEFI HTTP nativo, puede utilizar iPXE HTTP para el proceso de arranque.

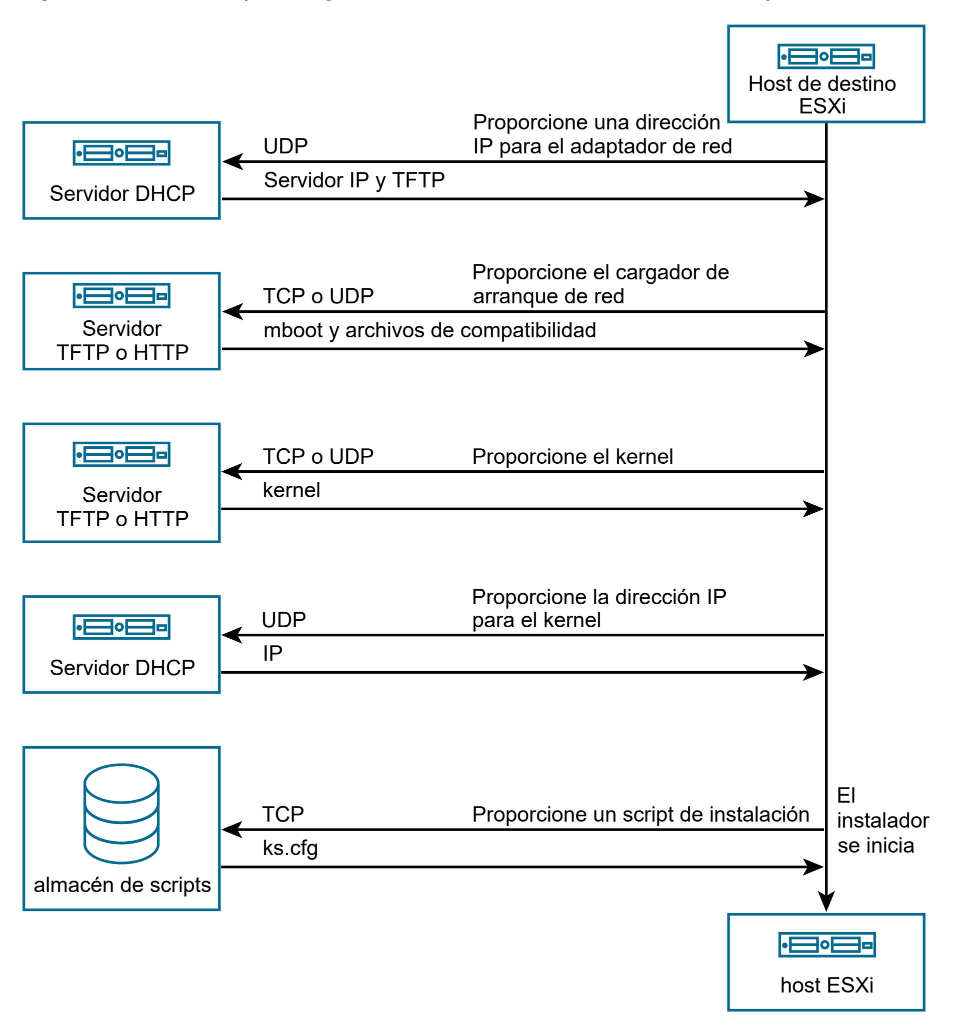
Nota El arranque de red con firmware de BIOS heredado solo se puede realizar mediante IPv4. El arranque de red con firmware de UEFI BIOS es posible a través de IPv4 o IPv6.

Descripción general de la instalación para el arranque de red

Puede arrancar un host ESXi desde una interfaz de red. Algunos de los detalles del proceso de arranque de red varían si el host de destino utiliza firmware de UEFI o BIOS heredado y si el proceso de arranque utiliza PXE TFTP, iPXE HTTP o UEFI HTTP.

Cuando se arranca un host de destino, este host interactúa con los diversos servidores en el entorno para obtener el adaptador de red, el cargador de arranque, el kernel, la dirección IP del kernel y, finalmente, un script de instalación. Una vez obtenidos todos los componentes, se inicia la instalación, como se muestra en la siguiente ilustración.

Figura 3-2. Descripción general de la instalación del arranque PXE



La interacción entre el host ESXi y los otros servidores continúa de la siguiente manera:

1 El usuario arranca el host ESXi de destino.

2 El host ESXi de destino realiza una solicitud DHCP.

3 El servidor DHCP responde con la información de IP, la ubicación del servidor TFTP o HTTP, y el nombre de archivo o la dirección URL del cargador de arranque de red inicial.

4 El host ESXi se pone contacto con el servidor TFTP o HTTP, y solicita el nombre de archivo o la URL que especificó el servidor DHCP.

5 El servidor TFTP o HTTP envía el cargador de arranque de red, y el host ESXi lo ejecuta. Es posible que el cargador de arranque inicial cargue componentes de cargador de arranque adicionales del servidor.

6 El cargador de arranque busca un archivo de configuración en el servidor TFTP o HTTP, descarga el kernel y otros componentes de ESXi según lo especificado en el archivo de configuración e inicia el kernel en el host ESXi.

7 El instalador se ejecuta de forma interactiva o mediante un script de inicio, según se especifique en el archivo de configuración.

Información sobre el arranque de red

Comprender el proceso de arranque de red puede ayudarle durante la solución de problemas.

Servidor TFTP

El protocolo trivial de transferencia de archivos (TFTP) es similar al servicio FTP y se utiliza generalmente solo para los sistemas de arranque de red o la carga de firmware en dispositivos de red, como los enrutadores. TFTP está disponible en Linux y Windows.

- La mayoría de las distribuciones de Linux incluyen una copia del servidor tftp-hpa. Si requiere una solución compatible, adquiera un servidor TFTP compatible de su proveedor de confianza. También puede adquirir un servidor TFTP desde uno de los dispositivos de paquete en VMware Marketplace.
- Si su servidor TFTP funciona en un host de Microsoft Windows, utilice tftpd32 versión 2.11 o una versión posterior. Consulte http://tftpd32.jounin.net/.

SYSLINUX y PXELINUX

Si utiliza PXE en un entorno BIOS heredado, debe comprender los distintos entornos de arranque.

- SYSLINUX es un entorno de arranque de código abierto para máquinas que ejecutan firmware de BIOS heredado. El cargador de arranque de ESXi para sistemas BIOS, `mboot.c32`, se ejecuta como un complemento de SYSLINUX. Puede configurar SYSLINUX para el arranque desde distintos tipos de medios, como un disco, una imagen ISO y una red. Puede encontrar el paquete de SYSLINUX en http://www.kernel.org/pub/linux/utils/boot/syslinux/.
- PXELINUX es una configuración de SYSXLINUX para realizar el arranque desde un servidor TFTP, según el estándar PXE. Si utiliza PXELINUX para arrancar el instalador de ESXi, el archivo binario `pxelinux.0`, `mboot.c32`, el archivo de configuración, el kernel y otros archivos se transfieren mediante TFTP.

Nota VMware compila el complemento `mboot.c32` para que funcione con la versión 3.86 de SYSLINUX y prueba el arranque PXE solo con esa versión. Otras versiones podrían ser incompatibles. *El paquete de divulgación de código abierto para VMware vSphere Hypervisor* incluye correcciones de errores para la versión 3.86 de SYSLINUX.

---

iPXE

iPXE es un software de código abierto que proporciona una implementación de HTTP. Puede utilizar el software para realizar un arranque inicial. Para obtener más información, consulte https://ipxe.org/.

VMware incluye una compilación de iPXE como parte de Auto Deploy. El árbol de origen de esta compilación está disponible en *el paquete de divulgación de código abierto para VMware vCenter Server*.

UEFI PXE y UEFI HTTP

La mayoría del firmware UEFI es compatible de forma nativa con PXE, lo que permite arrancar desde un servidor TFTP. El firmware puede cargar directamente el cargador de arranque de ESXi para los sistemas UEFI, `mboot.efi`. No es necesario ningún software adicional (p. ej., PXELINUX).

Algunos firmware UEFI son compatibles con el arranque HTTP UEFI nativo. La función se introdujo en la versión 2.5 de la especificación UEFI. El firmware puede cargar el cargador de arranque de ESXi desde un servidor HTTP, sin software adicional, como iPXE.

Nota Los productos Apple Macintosh no son compatibles con el arranque PXE. En cambio, son compatibles con el arranque de red mediante un protocolo específico para Apple.

Métodos alternativos para el arranque de red

También existen métodos alternativos para el arranque de red de software y hosts distintos, por ejemplo:

- Configuración del servidor DHCP para que proporcione diferentes nombres de archivo del cargador de arranque inicial a distintos hosts según la dirección MAC u otros criterios. Consulte la documentación del servidor DCHP.
- Métodos que utilizan iPXE como cargador de arranque inicial con un archivo de configuración de iPXE que selecciona el siguiente cargador de arranque según la dirección MAC u otros criterios.

Archivos de configuración PXELINUX

Se necesita un archivo de configuración PXELINUX para iniciar el instalador de ESXi en un sistema BIOS heredado. El archivo de configuración define el menú que se muestra en el host ESXi de destino a medida que se inicia.

En esta sección, se brinda información general sobre los archivos de configuración PXELINUX.

Para conocer detalles de la sintaxis, visite el sitio web de SYSLINUX en http://www.syslinux.org/.

Archivos requeridos

En el archivo de configuración de PXE, debe incluir rutas de acceso a los siguientes archivos:

- `mboot.c32` es el cargador de arranque.
- `boot.cfg` es el archivo de configuración del cargador de arranque.

Consulte Acerca del archivo boot.cfg .

Nombre del archivo de configuración de PXE

Para el nombre del archivo de configuración de PXE, seleccione una de las siguientes opciones:

- `01-`*`dirección_MAC_del_host_ESXi_de_destino`*. Por ejemplo, `01-23-45-67-89-0a-bc`
- La dirección IP del host ESXi de destino en anotación hexadecimal.
- `default`

El archivo de arranque inicial, `pxelinux.0`, intenta cargar un archivo de configuración de PXE en el siguiente orden:

1 Intenta con la dirección MAC del host ESXi de destino, con su código de tipo ARP, que es 01 para Ethernet, como prefijo.

2 Si ese intento genera un error, intenta con la anotación hexadecimal de la dirección IP del sistema ESXi de destino.

3 Por último, intenta cargar un archivo con el nombre `default`.

Ubicación del archivo de configuración de PXE

Guarde el archivo en `/tftpboot/pxelinux.cfg/` en el servidor TFTP.

Por ejemplo, es posible guardar el archivo en el servidor TFTP en `/tftpboot/pxelinux.cfg/01-00-21-5a-ce-40-f6`. La dirección MAC del adaptador de red del host ESXi de destino es 00-21-5a-ce-40-f6.

Arrancar el instalador de ESXi mediante PXE y TFTP

Es posible utilizar un servidor TFTP para arrancar con PXE el instalador de ESXi. El proceso varía levemente si se utiliza UEFI o el arranque desde un BIOS heredado.

- En los equipos con BIOS heredado, el procedimiento admite el arranque de varias versiones del instalador de ESXi con el mismo cargador de arranque inicial `pxelinux.0` para todos los equipos de destino, pero con archivos de configuración PXELINUX potencialmente diferentes según la dirección MAC de los equipos de destino.
- En los equipos con UEFI, el procedimiento admite el arranque de varias versiones diferentes del instalador de ESXi con el mismo cargador de arranque inicial `mboot.efi` para todos los equipos de destino, pero con archivos `boot.cfg` potencialmente diferentes según la dirección MAC de los equipos de destino.

Requisitos previos

Puesto que la mayoría de los entornos contienen tanto hosts ESXi compatibles con el arranque UEFI como hosts compatibles solo con el BIOS heredado, en este tema se analizan los requisitos previos y los pasos para ambos tipos de hosts.

Compruebe que el entorno cumpla con los siguientes requisitos previos.

- Imagen ISO del instalador de ESXi descargada del sitio web de VMware.

- Host de destino con una configuración de hardware que sea compatible con la versión de ESXi. Consulte la *Guía de compatibilidad de VMware*.
- Un adaptador de red compatible con PXE en el host ESXi de destino.
- Servidor DHCP que puede configurar para el arranque PXE. Consulte Configuraciones de DHCP de muestra.
- Servidor TFTP.
- Directivas de seguridad de red para permitir el tráfico TFTP (Puerto UDP 69).
- Para BIOS heredado, solo se pueden usar redes IPv4. Para el arranque PXE con UEFI, se pueden usar redes IPv4 o IPv6.
- (Opcional) Un script de instalación (archivo de inicio).
- En la mayoría de los casos debe usar una VLAN nativa. Si desea especificar el identificador de la VLAN que se va a utilizar con el arranque PXE, compruebe que su NIC admita la especificación de identificador de la VLAN.

Para los sistemas BIOS heredados, obtenga la versión 3.86 del paquete SYSLINUX. Para obtener más información, consulte Información sobre el arranque de red.

Procedimiento

1 Si el host ESXi ejecuta únicamente el firmware de BIOS heredado, obtenga y configure PXELINUX.

   a Obtenga la versión 3.86 de SYSLINUX, descomprima el paquete y copie el archivo `pxelinux.0` en el directorio de nivel superior `/tftpboot` de su servidor TFTP.

   b Cree un archivo de configuración PXELINUX con el siguiente modelo de código.

   `ESXi-8.x.x-XXXXXX` es el nombre del subdirectorio TFTP donde se encuentran los archivos del instalador de ESXi.

```
DEFAULT install
NOHALT 1
LABEL install
  KERNEL ESXi-8.x.x-XXXXXX/mboot.c32
  APPEND -c ESXi-8.x.x-XXXXXX/boot.cfg
  IPAPPEND 2
```

   c Guarde el archivo PXELINUX en el directorio `/tftpboot/pxelinux.cfg` de su servidor TFTP con un nombre de archivo que determine si todos los hosts arrancarán este instalador de forma predeterminada:

Opción	Descripción
Mismo instalador	Use el nombre `default` para el archivo si desea que todos los hosts arranquen este instalador de ESXi de forma predeterminada.
Diferentes instaladores	Use la dirección MAC del equipo host de destino (01-*dirección_MAC_del_host_ESXi_de_destino*) como nombre para el archivo si desea que solo un host específico arranque con este archivo (por ejemplo, `01-23-45-67-89-0a-bc`).

2 Si el host ESXi ejecuta firmware UEFI, copie los archivos `efi/boot/bootx64.efi` y `efi/boot/crypto64.efi` desde la imagen ISO del instalador de ESXi a la carpeta `/tftpboot` en el servidor TFTP.

3 Cambie el nombre del archivo `efi/boot/bootx64.efi` a `mboot.efi`.

   Nota Generalmente, las versiones más recientes de `mboot.efi` pueden arrancar versiones anteriores de ESXi, pero es posible que las versiones anteriores de `mboot.efi` no puedan arrancar versiones más recientes de ESXi. Si desea configurar diversos hosts de manera que arranquen diferentes versiones del instalador de ESXi, utilice el archivo `mboot.efi` de la versión más reciente.

4 Configure el servidor DHCP.

5 Cree un subdirectorio en el directorio de nivel superior del servidor TFTP `/tftpboot` con el nombre de la versión de ESXi que almacenará, por ejemplo, `/tftpboot/ESXi-8.x.x-xxxxx`.

6 Copie el contenido de la imagen del instalador de ESXi en el directorio que acaba de crear.

7 Modifique el archivo `boot.cfg`.

   a Agregue la siguiente línea:

   ```
   prefix=ESXi-7.x.x-xxxxxx
   ```

   Aquí, `ESXi-7.x.x-xxxxxx` es el nombre de la ruta de acceso de los archivos del instalador en el directorio raíz del servidor TFTP.

   b Si los nombres de archivo en las líneas `kernel=` y `modules=` comienzan con un carácter de barra diagonal (/), elimine ese carácter.

   c Si la línea de `kernelopt=` contiene la cadena `cdromBoot`, quite únicamente la cadena.

8 (opcional) En el caso de una instalación generada por script, en el archivo `boot.cfg`, agregue la opción `kernelopt` en la línea siguiente al comando del kernel, para especificar la ubicación del script de instalación.

   Utilice el siguiente código como modelo, donde `XXX.XXX.XXX.XXX` es la dirección IP del servidor en el que reside el script de instalación y `esxi_ksFiles` es el directorio que contiene el archivo `ks.cfg`.

   ```
   kernelopt=ks=http://XXX.XXX.XXX.XXX/esxi_ksFiles/ks.cfg
   ```

9 Si el host ESXi ejecuta el firmware UEFI, especifique si desea que todos los hosts UEFI arranquen el mismo instalador.

Opción	Descripción
Mismo instalador	Copie el archivo `boot.cfg` en `/tftpboot/boot.cfg` o vincúlelo a esta ruta.
Diferentes instaladores	a Cree un subdirectorio de `/tftpboot` con la dirección MAC del equipo host de destino (01-*dirección_MAC_del_host_ESXi_de_destino*) como nombre (por ejemplo, `01-23-45-67-89-0a-bc`). b Coloque una copia (o un vínculo) del archivo `boot.cfg` del host en ese directorio (por ejemplo, `/tftpboot/01-23-45-67-89-0a-bc/boot.cfg`).

Arrancar el instalador de ESXi mediante iPXE y HTTP

Puede usar iPXE para arrancar el instalador de ESXi desde un servidor HTTP.

- En los equipos con BIOS heredado, el procedimiento admite el arranque de varias versiones del instalador de ESXi con el mismo cargador de arranque inicial `pxelinux.0` para todos los equipos de destino, pero con archivos de configuración PXELINUX potencialmente diferentes según la dirección MAC de los equipos de destino.
- En los equipos con UEFI, el procedimiento admite el arranque de varias versiones diferentes del instalador de ESXi con el mismo cargador de arranque inicial `mboot.efi` para todos los equipos de destino, pero con archivos `boot.cfg` potencialmente diferentes según la dirección MAC de los equipos de destino.

Requisitos previos

Los requisitos previos y los pasos dependen solo de la compatibilidad con el arranque UEFI o el BIOS heredado. iPXE se puede utilizar para arrancar el instalador de ESXi desde un servidor HTTP. El siguiente tema analiza los requisitos previos y los pasos para hosts ESXi que admiten el arranque UEFI y los hosts que solo admiten la BIOS heredada.

Compruebe que el entorno tenga los siguientes componentes:

- Imagen ISO del instalador de ESXi descargada del sitio web de VMware.
- Host de destino con una configuración de hardware que sea compatible con la versión de ESXi. Consulte la *Guía de compatibilidad de VMware*.
- Un adaptador de red compatible con PXE en el host ESXi de destino.
- Servidor DHCP que puede configurar para el arranque PXE. Consulte Configuraciones de DHCP de muestra.
- Servidor TFTP.
- Directivas de seguridad de red para permitir el tráfico TFTP (Puerto UDP 69).
- Para BIOS heredado, solo se pueden usar redes IPv4. Para el arranque PXE con UEFI, se pueden usar redes IPv4 o IPv6.
- (Opcional) Un script de instalación (archivo de inicio).
- En la mayoría de los casos debe usar una VLAN nativa. Si desea especificar el identificador de la VLAN que se va a utilizar con el arranque PXE, compruebe que su NIC admita la especificación de identificador de la VLAN.

Asegúrese de que el entorno también cumpla los siguientes requisitos previos para el arranque PXE mediante un servidor HTTP:

- Compruebe que los hosts ESXi de destino puedan acceder al servidor HTTP.
- Si el host ESXi ejecuta únicamente el firmware de BIOS heredado, obtenga la versión 3.86 del paquete SYSLINUX. Para obtener más información, consulte Información sobre el arranque de red.

Procedimiento

1 Obtenga y configure iPXE.

a Obtenga el código fuente de iPXE.

b En la página de descarga de iPXE, siga las instrucciones de compilación, pero ejecute uno de los siguientes comandos.

- En el caso de los hosts ESXi que solo ejecutan el firmware de BIOS heredado, ejecute `make bin/undionly.kpxe`.
- Para los hosts ESXi que ejecuten el firmware UEFI, ejecute `make bin-x86_64-efi/snponly.efi`.

c Copie el archivo `undionly.kpxe` o `snponly.efi` al directorio `/tftpboot` del servidor TFTP.

2 Si el host ESXi ejecuta únicamente el firmware de BIOS heredado, obtenga y configure PXELINUX.

a Obtenga la versión 3.86 de SYSLINUX, descomprima el paquete y copie el archivo `pxelinux.0` en el directorio `/tftpboot` de su servidor TFTP.

b Cree un archivo de configuración PXELINUX con el siguiente modelo de código.

`ESXi-8.x.x-XXXXXX` es el nombre del subdirectorio TFTP donde se encuentran los archivos del instalador de ESXi.

```
DEFAULT install
NOHALT 1
LABEL install
  KERNEL ESXi-8.x.x-XXXXXX/mboot.c32
  APPEND -c ESXi-8.x.x-XXXXXX/boot.cfg
  IPAPPEND 2
```

c Guarde el archivo PXELINUX en el directorio `/tftpboot/pxelinux.cfg` del servidor TFTP.

El nombre de archivo determina si todos los hosts arrancarán este instalador de forma predeterminada.

Opción	Descripción
Mismo instalador	Use el nombre `default` para el archivo si desea que todos los hosts arranquen este instalador de ESXi de forma predeterminada.
Diferentes instaladores	Asigne un nombre al archivo con la dirección MAC del equipo host de destino (01-*dirección_mac_de_host_ESXi_destino*), si solo un host específico debe arrancar este archivo. Por ejemplo, `01-23-45-67-89-0a-bc`.

3 Si el host ESXi ejecuta el firmware UEFI, copie el archivo `efi/boot/bootx64.efi` desde la imagen ISO del instalador de ESXi en la carpeta `/tftpboot` del servidor TFTP y cambie el nombre del archivo a `mboot.efi`.

Nota Generalmente, las versiones más recientes de `mboot.efi` pueden arrancar versiones anteriores de ESXi, pero es posible que las versiones anteriores de `mboot.efi` no puedan arrancar versiones más recientes de ESXi. Si desea configurar diversos hosts de manera que arranquen diferentes versiones del instalador de ESXi, utilice el archivo `mboot.efi` de la versión más reciente.

4 Configure el servidor DHCP.

5 Cree un directorio en el servidor HTTP que tenga el mismo nombre que la versión de ESXi que contendrá. Por ejemplo, `/var/www/html/ESXi-8.x.x-XXXXXX`.

6 Copie el contenido de la imagen del instalador de ESXi en el directorio que acaba de crear.

7 Modifique el archivo `boot.cfg`.

   a Agregue la siguiente línea:

   ```
   prefix=http://XXX.XXX.XXX.XXX/ESXi-8.x.x-XXXXXX
   ```

   En la línea superior, `http://XXX.XXX.XXX.XXX/ESXi-8.x.x-XXXXXX` es la ubicación de los archivos del instalador en el servidor HTTP.

   b Si los nombres de archivo en las líneas `kernel=` y `modules=` comienzan con un carácter de barra diagonal (/), elimine ese carácter.

   c Si la línea de `kernelopt=` contiene la cadena `cdromBoot`, quite únicamente la cadena.

8 (opcional) En el caso de una instalación generada por script, en el archivo `boot.cfg`, agregue la opción `kernelopt` en la línea siguiente al comando del kernel, para especificar la ubicación del script de instalación.

Utilice el siguiente código como modelo, donde `XXX.XXX.XXX.XXX` es la dirección IP del servidor en el que reside el script de instalación y `esxi_ksFiles` es el directorio que contiene el archivo `ks.cfg`.

```
kernelopt=ks=http://XXX.XXX.XXX.XXX/esxi_ksFiles/ks.cfg
```

9 Si el host ESXi ejecuta el firmware UEFI, especifique si desea que todos los hosts UEFI arranquen el mismo instalador.

Opción	Descripción
Mismo instalador	Copie el archivo `boot.cfg` en `/tftpboot/boot.cfg` o vincúlelo a esta ruta.
Diferentes instaladores	a Cree un subdirectorio de `/tftpboot` con la dirección MAC del equipo host de destino (01-*dirección_MAC_del_host_ESXi_de_destino*) como nombre (por ejemplo, `01-23-45-67-89-0a-bc`). b Coloque una copia (o un vínculo) del archivo `boot.cfg` del host en ese directorio (por ejemplo, `/tftpboot/01-23-45-67-89-0a-bc/boot.cfg`).

Arrancar el instalador de ESXi mediante HTTP de UEFI nativo

El instalador de ESXi se puede arrancar directamente desde un servidor HTTP, sin necesidad de disponer de software adicional para admitir el proceso.

HTTP de UEFI permite arrancar varias versiones del instalador de ESXi. Se utiliza el mismo cargador de arranque inicial `mboot.efi` para todos los equipos de destino, pero potencialmente diferentes archivos `boot.cfg` en función de la dirección MAC del equipo de destino.

Nota No mezcle las redes IPv4 o IPv6 durante el proceso de arranque. Utilice solo una de ellas.

Requisitos previos

Compruebe que el entorno tenga los siguientes componentes:

- Un host ESXi con firmware UEFI que admita la función de arranque HTTP.
- Imagen ISO del instalador de ESXi descargada del sitio web de VMware.
- Host de destino con una configuración de hardware que sea compatible con la versión de ESXi. Consulte la *Guía de compatibilidad de VMware*.
- Un adaptador de red compatible con redes UEFI en el host ESXi de destino.
- Un servidor DHCP que podrá configurar para el arranque HTTP de UEFI. Consulte Configuraciones de DHCP de muestra.
- (Opcional) Un script de instalación (archivo de inicio).
- En la mayoría de los casos debe usar una VLAN nativa. Si desea especificar el identificador de la VLAN que se va a utilizar con el arranque PXE, compruebe que su NIC admita la especificación de identificador de la VLAN.

Procedimiento

1 Copie el archivo `efi/boot/bootx64.efi` desde la imagen ISO del instalador de ESXi en un directorio del servidor HTTP y cambie el nombre del archivo a `mboot.efi`. Por ejemplo, `http://www.example.com/esxi/mboot.efi`.

   Nota Generalmente, las versiones más recientes de `mboot.efi` pueden arrancar versiones anteriores de ESXi, pero es posible que las versiones anteriores de `mboot.efi` no puedan arrancar versiones más recientes de ESXi. Si desea configurar diversos hosts de manera que arranquen diferentes versiones del instalador de ESXi, utilice el archivo `mboot.efi` de la versión más reciente.

2 Configure el servidor DHCP.

3 Cree un directorio en el servidor HTTP que tenga el mismo nombre que la versión de ESXi que contendrá. Por ejemplo, `http://www.example.com/esxi/ESXi-8.x.x-XXXXXX`.

4 Copie el contenido de la imagen del instalador de ESXi en el directorio que acaba de crear.

5 Modifique el archivo `boot.cfg`.

   a Agregue la siguiente línea con la dirección URL del directorio que acaba de crear.

   ```
   prefix=http://www.example.com/esxi/ESXi-8.x.x-XXXXXX
   ```

   b Si los nombres de archivo en las líneas `kernel=` y `modules=` comienzan con un carácter de barra diagonal (/), elimine ese carácter.

   c Si la línea de `kernelopt=` contiene la cadena `cdromBoot`, quite únicamente la cadena.

6 (opcional) En el caso de una instalación generada por script, en el archivo `boot.cfg`, agregue la opción `kernelopt` en la línea siguiente al comando del kernel, para especificar la ubicación del script de instalación.

   Por ejemplo, `kernelopt=ks=http://www.example.com/esxi_ksFiles/ks.cfg`

7 (opcional) Puede utilizar los parámetros de configuración de la máquina virtual *networkBootProtocol* y *networkBootUri* para especificar desde dónde se puede arrancar una máquina virtual. La opción *networkBootProtocol* especifica el protocolo de arranque, IPv4 o IPv6. Por ejemplo, `networkBootProtocol = httpv4`. La opción *networkBootUri* especifica la URL HTTP del cargador de arranque ESXi (bootx64.efi). Por ejemplo, `networkBootUri = http://xxx.xxx.xx.x/esxi80uc1/efi/boot/bootx64.efi`.

8 Especifique si desea que todos los hosts UEFI arranquen el mismo instalador.

Opción	Descripción
Mismo instalador	Agregue el archivo `boot.cfg` al mismo directorio que `mboot.efi`. Por ejemplo, `http://www.example.com/esxi/boot.cfg`
Diferentes instaladores	a Cree un subdirectorio del directorio que contenga el archivo `mboot.efi`. Asigne un nombre al directorio que sea como la dirección MAC del equipo host de destino (01-*dirección_mac_de_host_ESXi_destino*); por ejemplo, `01-23-45-67-89-0a-bc`. b Agregue el archivo `boot.cfg` personalizado al directorio. Por ejemplo, `http://www.example.com/esxi/01-23-45-67-89-0a-bc/boot.cfg`.

Puede utilizar ambos tipos de instalador. Los hosts ESXi que no tengan un archivo `boot.cfg` personalizado en el servidor HTTP, arranque desde el archivo `boot.cfg` predeterminado.

Configuraciones de DHCP de muestra

El servidor DHCP debe enviar la dirección del servidor TFTP o HTTP, y el nombre de archivo del cargador de arranque inicial al host ESXi.

Cuando la máquina de destino arranca por primera vez, transmite un paquete mediante la red para solicitar información a fin de realizar el arranque por sí misma. El servidor DHCP responde. El servidor DHCP debe ser capaz de determinar si la máquina de destino puede arrancar y, asimismo, de determinar la ubicación del archivo binario del cargador de arranque inicial. Para el arranque PXE, la ubicación es un archivo en un servidor TFTP. Para el arranque UEFI HTTP, la ubicación es una URL.

Precaución No configure un segundo servidor DHCP si la red ya tiene uno. Si varios servidores DHCP responden a las solicitudes de DHCP, las máquinas pueden obtener direcciones IP incorrectas o en conflicto, o no recibir la información de arranque correcta. Consulte a un administrador de red antes de configurar un servidor DHCP. Para obtener asistencia en relación con la configuración de DHCP, póngase en contacto con el proveedor del servidor DHCP.

Hay muchos servidores DHCP que puede utilizar. Los siguientes ejemplos son para un servidor DHCP de ISC. Si usa una versión de DHCP para Microsoft Windows, consulte la documentación del servidor DHCP para determinar cómo transmitir los argumentos `next-server` y `filename` a la máquina de destino.

Ejemplo de arranque mediante PXE y TFTP con IPv4

En este ejemplo se muestra cómo configurar un servidor DHCP de ISC para el arranque PXE de ESXi mediante un servidor TFTP en una dirección IPv4 xxx.xxx.xxx.xxx.

```
#
# ISC DHCP server configuration file snippet.  This is not a complete
# configuration file; see the ISC server documentation for details on
# how to configure the DHCP server.
#
allow booting;
```

```
allow bootp;
option client-system-arch code 93 = unsigned integer 16;
class "pxeclients" {
   match if substring(option vendor-class-identifier, 0, 9) = "PXEClient";
   next-server xxx.xxx.xxx.xxx;
   if option client-system-arch = 00:07 or option client-system-arch = 00:09 {
      filename = "mboot.efi";
   } else {
      filename = "pxelinux.0";
   }
}
```

Cuando una máquina intenta realizar un arranque PXE, el servidor DHCP proporciona una dirección IP y la ubicación del archivo binario `pxelinux.0` o `mboot.efi` en el servidor TFTP.

Ejemplo de arranque mediante PXE y TFTP con IPv6

En este ejemplo se muestra cómo configurar un servidor DHCPv6 de ISC para el arranque PXE de ESXi mediante un servidor TFTP en una dirección IPv6 xxxx:xxxx:xxxx:xxxx::xxxx.

```
#
# ISC DHCPv6 server configuration file snippet.  This is not a complete
# configuration file; see the ISC server documentation for details on
# how to configure the DHCP server.
#
allow booting;
allow bootp;
option dhcp6.bootfile-url code 59 = string;
option dhcp6.bootfile-url "tftp://[xxxx:xxxx:xxxx:xxxx::xxxx]/mboot.efi";
```

Cuando una máquina intenta realizar un arranque PXE, el servidor DHCP proporciona una dirección IP y la ubicación del archivo binario `mboot.efi` en el servidor TFTP.

Ejemplo de arranque mediante iPXE y HTTP con IPv4

En este ejemplo se muestra cómo configurar un servidor DHCP de ISC para arrancar ESXi mediante la carga de iPXE desde un servidor TFTP en una dirección IPv4 `xxx.xxx.xxx.xxx`.

```
#
# ISC DHCP server configuration file snippet.  This is not a complete
# configuration file; see the ISC server documentation for details on
# how to configure the DHCP server.
#
allow booting;
allow bootp;
option client-system-arch code 93 = unsigned integer 16;
class "pxeclients" {
   match if substring(option vendor-class-identifier, 0, 9) = "PXEClient";
   next-server xxx.xxx.xxx.xxx;
   if option client-system-arch = 00:07 or option client-system-arch = 00:09 {
      if exists user-class and option user-class = "iPXE" {
         # Instruct iPXE to load mboot.efi as secondary bootloader
         filename = "mboot.efi";
```

```
      } else {
         # Load the snponly.efi configuration of iPXE as initial bootloader
         filename = "snponly.efi";
      }
   } else {
      if exists user-class and option user-class = "iPXE" {
         # Instruct iPXE to load pxelinux as secondary bootloader
         filename = "pxelinux.0";
      } else {
         # Load the undionly configuration of iPXE as initial bootloader
         filename = "undionly.kpxe";
   }
}
```

Cuando una máquina intenta realizar un arranque PXE, el servidor DHCP proporciona una dirección IP y la ubicación del archivo binario `undionly.kpxe` o `snponly.efi` en el servidor TFTP. En el caso de BIOS heredado, iPXE pide al servidor DHCP el siguiente archivo que se debe cargar y el servidor devuelve el nombre de archivo `pxelinux.0`. En el caso de UEFI, iPXE pide al servidor DHCP el siguiente archivo que se debe cargar y, en esta ocasión, el servidor devuelve el nombre de archivo `mboot.efi`. En ambos casos, iPXE es residente, y el sistema tiene la capacidad HTTP. Como resultado, el sistema puede cargar archivos adicionales desde un servidor HTTP.

Ejemplo de arranque mediante iPXE y HTTP con IPv6

En este ejemplo se muestra cómo configurar un servidor DHCPv6 de ISC para arrancar ESXi mediante la carga de iPXE desde un servidor TFTP en una dirección IPv6 `xxxx:xxxx:xxxx:xxxx::xxxx`.

```
#
# ISC DHCPv6 server configuration file snippet.  This is not a complete
# configuration file; see the ISC server documentation for details on
# how to configure the DHCP server.
#
allow booting;
allow bootp;

option dhcp6.bootfile-url code 59 = string;
if exists user-class and option user-class = "iPXE" {
   # Instruct iPXE to load mboot.efi as secondary bootloader
   option dhcp6.bootfile-url "tftp://[xxxx:xxxx:xxxx:xxxx::xxxx]/mboot.efi";
} else {
   # Load the snponly.efi configuration of iPXE as initial bootloader
   option dhcp6.bootfile-url "tftp://[xxxx:xxxx:xxxx:xxxx::xxxx]/snponly.efi";
}
```

Cuando una máquina intenta realizar un arranque PXE, el servidor DHCP proporciona una dirección IP y la ubicación del archivo binario `snponly.efi` (iPXE) en el servidor TFTP. iPXE pide al servidor DHCP el siguiente archivo que se debe cargar y, en esta ocasión, el servidor devuelve el nombre de archivo `mboot.efi`. iPXE es residente y el sistema tiene la capacidad HTTP. Como resultado, el sistema puede cargar archivos adicionales desde un servidor HTTP.

Ejemplo de arranque mediante UEFI HTTP con IPv4

En este ejemplo se muestra cómo configurar un servidor DHCP de ISC para arrancar ESXi mediante el uso de UEFI HTTP nativo en IPv4 desde el servidor web `www.example.com`.

```
#
# ISC DHCP server configuration file snippet.  This is not a complete
# configuration file; see the ISC server documentation for details on
# how to configure the DHCP server.
#
allow booting;
allow bootp;
option client-system-arch code 93 = unsigned integer 16;
class "httpclients" {
   match if substring(option vendor-class-identifier, 0, 10) = "HTTPClient";
   option vendor-class-identifier "HTTPClient";

   if option client-system-arch = 00:10 {
      # x86_64 UEFI HTTP client
      filename = http://www.example.com/esxi/mboot.efi;
   }
}
```

Ejemplo de arranque mediante UEFI HTTP con IPv6

En este ejemplo se muestra cómo configurar un servidor DHCPv6 de ISC para que arranque ESXi mediante el uso de HTTP UEFI nativo en IPv6 desde el servidor web `www.example.com`.

```
#
# ISC DHCPv6 server configuration file snippet.  This is not a complete
# configuration file; see the ISC server documentation for details on
# how to configure the DHCP server.
#
allow booting;
allow bootp;

option dhcp6.bootfile-url code 59 = string;
option dhcp6.user-class code 15 = { integer 16, string };
option dhcp6.vendor-class code 16 = { integer 32, integer 16, string };

if option dhcp6.client-arch-type = 00:10 {
      # x86_64 HTTP clients
      option dhcp6.vendor-class 0 10 "HTTPClient";
      option dhcp6.bootfile-url "http://www.example.com/esxi/mboot.efi";
}
```

Cómo actualizar hosts mediante comandos ESXCLI

Actualizar los hosts a través de comandos ESXCLI

Mediante el uso de ESXCLI, se puede actualizar un host ESXi 6.7 o ESXi 7.0 a la versión 8.0 y actualizar o revisar los hosts ESXi 6.7, ESXi 7.0 y ESXi 8.0.

vSphere 8.0 incluye archivos de configuración, componentes, imágenes base y complementos como nuevas entregas de software que se pueden utilizar para actualizar o aplicar revisiones a hosts ESXi 8.0. Para obtener información sobre la administración de componentes, imágenes base y complementos en ESXi, consulte Conceptos y ejemplos de ESXCLI.

Para usar los comandos ESXCLI, debe instalar una instancia de ESXCLI independiente. Para obtener más información sobre la instalación y el uso de ESXCLI, consulte los siguientes documentos.

- Uso de ESXCLI
- Introducción a ESXCLI
- Referencia de ESXCLI

Nota Si presiona Ctrl+C mientras se ejecuta un comando de `esxcli`, la interfaz de la línea de comandos se cierra y aparece un nuevo símbolo del sistema sin mostrar mensajes. Sin embargo, el comando continúa ejecutándose hasta la finalización.

Para hosts ESXi implementados con vSphere Auto Deploy, el VIB de herramientas debe formar parte de la imagen base de arranque que se utiliza para la instalación inicial de Auto Deploy. El VIB de herramientas no se puede agregar por separado más adelante.

VIB, perfiles de imagen y almacenes de software

La actualización de ESXi con comandos esxcli requiere comprender los VIB, los perfiles de imagen y los almacenes de software.

Los siguientes términos técnicos se utilizan en toda la documentación de vSphere en asuntos relacionados con tareas de instalación y actualización.

VIB

Un VIB es un paquete de software de ESXi. VMware y sus soluciones de paquetes de partners, controladores, proveedores de CIM y aplicaciones que extienden la plataforma de ESXi como VIB. Los VIB están disponibles en almacenes de software. Puede usar VIB para crear y personalizar imágenes ISO o para actualizar hosts ESXi mediante la instalación de VIB de forma asincrónica en los hosts.

Perfil de imagen

Un perfil de imagen define una imagen de ESXi y consta de VIB. Un perfil de imagen incluye un VIB base y también podría incluir más VIB. Es posible analizar y definir un perfil de imagen mediante vSphere ESXi Image Builder.

Almacén de software

Un almacén de software es una colección de VIB y perfiles de imagen. El almacén de software es una jerarquía de archivos y carpetas, y puede estar disponible a través de una URL HTTP (almacén en línea) o un archivo ZIP (almacén sin conexión). Los partners VMware y VMware se encargan de que los almacenes estén disponibles. Las compañías con instalaciones de VMware grandes podrían crear almacenes internos para aprovisionar hosts ESXi con vSphere Auto Deploy o para exportar un imagen ISO para la instalación de ESXi.

Información sobre los niveles de aceptación para los VIB y hosts

Cada VIB se lanza con un nivel de aceptación que no se puede cambiar. El nivel de aceptación del host determina qué VIB pueden instalarse en un host.

El nivel de aceptación se aplica a los VIB individuales instalados mediante los comandos `esxcli software vib install` y `esxcli software vib update`, a los VIB instalados mediante vSphere Lifecycle Manager y a los VIB de los perfiles de imagen.

El nivel de aceptación de todos los VIB de un host debe ser, como mínimo, tan alto como el nivel de aceptación del host. Por ejemplo, si el nivel de aceptación del host es VMwareAccepted, se pueden instalar VIB con los niveles de aceptación VMwareCertified y VMwareAccepted, pero no se pueden instalar VIB con los niveles de aceptación PartnerSupported o CommunitySupported. Para instalar un VIB con un nivel de aceptación menos restrictivo que el del host, puede cambiar la configuración del host mediante vSphere Client o ejecutando los comandos `esxcli software acceptance`.

La configuración de los niveles de aceptación de los hosts es una práctica recomendada que le permite especificar qué VIB pueden instalarse en un host y utilizarse con un perfil de imagen, y el nivel de compatibilidad que puede esperarse para un VIB. Por ejemplo, puede configurar un nivel de aceptación más restrictivo para los hosts de un entorno de producción que para los hosts de un entorno de prueba.

VMware admite los siguientes niveles de aceptación.

VMwareCertified

El nivel de aceptación VMwareCertified tiene los requisitos más estrictos. Los VIB con este nivel se someten a pruebas completamente equivalentes a las pruebas de control de calidad internas de VMware para la misma tecnología. Hoy en día, solo los controladores de los programas de proveedores de E/S (I/O Vendor Program, IOVP) se publican en este nivel. VMware responde a las llamadas de soporte para VIB con este nivel de aceptación.

VMwareAccepted

Los VIB con este nivel de aceptación pasan por pruebas de comprobación, pero estas no prueban completamente todas las funciones del software. El partner realiza pruebas y VMware comprueba el resultado. Hoy en día, los proveedores de CIM y los complementos de PSA son algunos de los VIB que se publican en este nivel. VMware indica a los clientes que realizan llamadas de soporte para VIB con este nivel de aceptación que se pongan en contacto con la organización de soporte del partner.

PartnerSupported

Los VIB con el nivel de aceptación PartnerSupported los publica un partner de confianza de VMware. El partner realiza todas las pruebas. VMware no comprueba los resultados. Este nivel se utiliza para una tecnología nueva o alternativa que los partners desean habilitar para los sistemas VMware. Hoy en día, las tecnologías de VIB de controlador, como Infiniband, ATAoE y SSD, se encuentran en este nivel con controladores de hardware que no son estándar. VMware indica a los clientes que realizan llamadas de soporte para VIB con este nivel de aceptación que se pongan en contacto con la organización de soporte del partner.

CommunitySupported

El nivel de aceptación CommunitySupported es para VIB creados por personas o empresas por fuera de los programas de partners de VMware. Los VIB de este nivel de aceptación no pasaron por un programa de pruebas aprobado por VMware y no son compatibles con el soporte técnico de VMware ni los partners de VMware.

Tabla 3-10. Niveles de aceptación de VIB necesarios para la instalación en hosts

Nivel de aceptación de host	VIB VMwareCertified	VIB VMwareAccepted	VIB PartnerSupported	VIB CommunitySupported
VMwareCertified	x			
VMwareAccepted	x	x		
PartnerSupported	x	x	x	
CommunitySupported	x	x	x	x

Equiparar un nivel de aceptación de un host con un nivel de aceptación de una actualización

Puede cambiar el nivel de aceptación de un host para que coincida con el nivel de aceptación de una actualización para un VIB o un perfil de imagen que desee instalar. El nivel de aceptación de todos los VIB de un host debe ser, como mínimo, tan alto como el nivel de aceptación del host.

Use este procedimiento para determinar los niveles de aceptación del host y el VIB o el perfil de imagen que desea instalar y para cambiar el nivel de aceptación del host, si es necesario para la actualización.

Cuando se especifica un servidor de destino mediante `--server=<server_name>`, el servidor le solicita un nombre de usuario y una contraseña. Se admiten otras opciones de conexión, como un archivo de configuración o un archivo de sesión. Para obtener una lista de opciones de conexión, consulte Introducción a ESXCLI o ejecute `esxcli --help` en el símbolo del sistema de ESXCLI.

Requisitos previos

Instale ESXCLI. Consulte Introducción a ESXCLI. Para solucionar problemas, ejecute comandos `esxcli` en ESXi Shell.

Procedimiento

1 Recupere el nivel de aceptación del VIB o el perfil de imagen.

Opción	Descripción
Mostrar información para todos los VIB	esxcli --server=<*nombre_del_servidor*> software sources vib list --depot=<*URL_del_almacén*>
Mostrar información para un VIB especificado	esxcli --server=<*nombre_del_servidor*> software sources vib list --viburl=<*url_del_VIB*>
Mostrar información para todos los perfiles de imagen	esxcli --server=<*nombre_del_servidor*> software sources profile list --depot=<*URL_del_almacén*>
Mostrar información para un perfil de imagen especificado	esxcli --server=<*nombre_del_servidor*> software sources profile get --depot=<*URL_del_almacén*> --profile=<*nombre_del_perfil*>

2 Recupere el nivel de aceptación del host.

```
esxcli --server=<nombre_del_servidor> software acceptance get
```

3 (opcional) Si el nivel de aceptación del VIB es más restrictivo que el nivel de aceptación del host, cambie el nivel de aceptación del host.

```
esxcli --server=<nombre_del_servidor> software acceptance set --level=<nivel_de_aceptación>
```

El parámetro *acceptance_level* puede ser `VMwareCertified`, `VMwareAccepted`, `PartnerSupported` o `CommunitySupported`. Los valores para *nivel_de_aceptación* distinguen mayúsculas de minúsculas.

Nota Puede usar la opción `--force` en el comando `esxcli software vib` o `esxcli software profile` para agregar un VIB o un perfil de imagen con un nivel de aceptación inferior al del host. Aparecerá un mensaje de advertencia. Debido a que la configuración ya no es coherente, el mensaje de advertencia se repetirá al instalar VIB, quitar VIB y realizar algunas otras operaciones en el host.

Ver si la actualización de host ESXi requiere el modo de mantenimiento o el reinicio

Los VIB que instala con la instalación en vivo no requieren el reinicio del host, pero es posible que requieran que el host se coloque en el modo de mantenimiento.

Cuando se especifica un servidor de destino mediante `--server=<server_name>`, el servidor le solicita un nombre de usuario y una contraseña. Se admiten otras opciones de conexión, como un archivo de configuración o un archivo de sesión. Para obtener una lista de opciones de conexión, consulte Introducción a ESXCLI o ejecute `esxcli --help` en el símbolo del sistema de ESXCLI.

Requisitos previos

Otros VIB y perfiles podrían requerir que el host se reinicie después de la instalación o actualización.

Instale ESXCLI. Consulte Introducción a ESXCLI. Para solucionar problemas, ejecute comandos `esxcli` en ESXi Shell.

Procedimiento

1 Compruebe si el VIB o el perfil de imagen que desea instalar requiere que el host se coloque en el modo de mantenimiento o se reinicie después de la instalación o actualización.

Ejecute uno de los siguientes comandos.

Opción	Descripción
Comprobar VIB	`esxcli --server=<server_name> software sources vib get -v <absolute_path_to_vib>`
Comprobar VIB en un almacén	`esxcli --server=<server_name> software sources vib get --depot=<depot_name>`
Comprobar perfil de imagen en un almacén	`esxcli --server=<server_name> software sources profile get --depot=<depot_name>`

2 Examine los valores de retorno.

Los valores de retorno, que se leen desde los metadatos del VIB, indican si el host debe estar en el modo de mantenimiento antes de instalar el VIB o el perfil de imagen y si la instalación del VIB o perfil requiere el reinicio del host.

Nota vSphere Lifecycle Manager emplea una API de exploración de software de ESXi interna para determinar si se requiere o no el modo de mantenimiento. Cuando instala un VIB en un sistema en vivo, si el valor para `Live-Install-Allowed` se establece en falso, el resultado de la instalación instruye a vSphere Lifecycle Manager a reiniciar el host. Cuando quita un VIB de un sistema en vivo, si el valor para `Live-Remove-Allowed` se estableció en falso, el resultado de la eliminación instruye a vSphere Lifecycle Manager a reiniciar el host. En cualquier caso, cuando se inicia la corrección, vSphere Lifecycle Manager pone automáticamente el host en modo de mantenimiento.

Pasos siguientes

De ser necesario, coloque al host en el modo de mantenimiento. Consulte Poner un host en modo de mantenimiento. Si se requiere un reinicio y si el host pertenece a un clúster de VMware HA, elimine el host del clúster o deshabilite HA en el clúster antes de realizar la instalación o actualización. Además, ponga el host en modo de mantenimiento para minimizar la actividad del disco de arranque durante la actualización.

Poner un host en modo de mantenimiento

Algunas operaciones de instalación y actualización que utilizan la instalación directa requieren que el host se encuentre en modo de mantenimiento.

Se requiere el modo de mantenimiento cuando una operación de actualización debe reiniciarse. Sin embargo, solo debe poner el host en modo de mantenimiento de forma manual cuando use comandos esxcli para realizar operaciones de actualización.

Para determinar si una operación de actualización requiere que el host se encuentre en modo de mantenimiento, consulte Ver si la actualización de host ESXi requiere el modo de mantenimiento o el reinicio

---

Nota Si el host es miembro de un clúster de vSAN y algún objeto de la máquina virtual en el host utiliza la configuración Cantidad de errores que se tolerarán=0 en su directiva de almacenamiento, el host podría sufrir retrasos inusuales al entrar en modo de mantenimiento. El retraso ocurre porque vSAN debe evacuar este objeto del host para que la operación de mantenimiento se complete correctamente.

Cuando se especifica un servidor de destino mediante --server=<server_name>, el servidor le solicita un nombre de usuario y una contraseña. Se admiten otras opciones de conexión, como un archivo de configuración o un archivo de sesión. Para obtener una lista de opciones de conexión, consulte Introducción a ESXCLI o ejecute `esxcli --help` en el símbolo del sistema de ESXCLI.

Requisitos previos

Instale ESXCLI. Consulte Introducción a ESXCLI. Para solucionar problemas, ejecute comandos `esxcli` en ESXi Shell.

Procedimiento

1 Compruebe si el host está en modo de mantenimiento.

```
esxcli --server=<server_name> system maintenanceMode get
```

2 Apague cada máquina virtual que se ejecuta en el host ESXi.

Nota Puede enumerar todas las máquinas virtuales en ejecución y recuperar el identificador de ámbito de cada una ejecutando el siguiente comando.

```
esxcli --server=<server_name> vm process list
```

Opción	Comando
Para desactivar el sistema operativo invitado y luego apagar la máquina virtual	`esxcli --server=<server_name> vm process kill --type soft --world-id <vm_ID>`
Para apagar inmediatamente la máquina virtual	`esxcli --server=<server_name> vm process kill --type hard --world-id <vm_ID>`
Para forzar la operación de apagado	`esxcli --server=<server_name> vm process kill --type force --world-id <vm_ID>`

Como alternativa, para evitar apagar las máquinas virtuales, se las puede migrar a otro host. Consulte el tema Migrar máquinas virtuales en la documentación de *Administrar vCenter Server y hosts*.

3 Coloque el host en modo de mantenimiento.

```
esxcli --server=<server_name> system maintenanceMode set --enable true
```

4 Compruebe que el host esté en modo de mantenimiento.

```
esxcli --server=<server_name> system maintenanceMode get
```

Actualizar un host con VIB individuales

Puede actualizar un host con VIB almacenados en un almacén de software accesible a través de una URL o en un almacén de archivos ZIP sin conexión.

Importante Si va a actualizar ESXi a partir de un paquete de archivos ZIP de un almacén suministrado por VMware, ya sea en línea desde el sitio web de VMware o descargado localmente, VMware solo admite el método de actualización para almacenes suministrados por VMware especificado en el tema Actualizar un host con perfiles de imagen .

Nota Los comandos `esxcli software vib update` y `esxcli software vib install` no son compatibles con las operaciones de actualización. Consulte Actualizar un host con perfiles de imagen .

Cuando se especifica un servidor de destino mediante --server=<*server_name*>, el servidor le solicita un nombre de usuario y una contraseña. Se admiten otras opciones de conexión, como un archivo de configuración o un archivo de sesión. Para obtener una lista de opciones de conexión, consulte Introducción a ESXCLI o ejecute esxcli --help en el símbolo del sistema de ESXCLI.

Requisitos previos

- Instale ESXCLI. Consulte Introducción a ESXCLI. Para solucionar problemas, ejecute comandos esxcli en ESXi Shell.
- Determine si una actualización requiere que el host se encuentre en el modo de mantenimiento o se reinicie. De ser necesario, coloque al host en el modo de mantenimiento.

  Consulte Ver si la actualización de host ESXi requiere el modo de mantenimiento o el reinicio. Consulte Poner un host en modo de mantenimiento.
- Si la actualización requiere un reinicio y si el host pertenece a un clúster de vSphere HA, quite el host del clúster o desactive HA en el clúster.

Procedimiento

1 Determine qué VIB están instalados en el host.

```
esxcli --server=<server_name> software vib list
```

2 Conozca qué VIB están disponibles en el almacén.

Opción	Descripción
Desde un almacén accesible mediante URL	esxcli --server=<*server_name*> software sources vib list --depot=http://<*web_server*>/<*depot_name*>
Desde un archivo ZIP de almacén local	esxcli --server=<*server_name*> software sources vib list --depot=<*absolute_path_to_depot_zip_file*>

Puede especificar un servidor proxy mediante la opción --proxy.

3 Actualice los VIB existentes para incluir los VIB en el almacén o instalar nuevos VIB.

Opción	Descripción
Actualizar VIB desde un almacén accesible mediante URL	`esxcli --server=<server_name> software vib update --depot=http://<web_server>/<depot_name>`
Actualizar VIB desde un archivo ZIP de almacén local	`esxcli --server=<server_name> software vib update --depot=<absolute_path_to_depot_ZIP_file>`
Instalar todos los VIB desde un archivo ZIP de un almacén sin conexión específico (incluye VIB de VMware y VIB suministrados por un partner)	`esxcli --server=<server_name> software vib install --depot <path_to_VMware_vib_ZIP_file>\<VMware_vib_ZIP_file> --depot <path_to_partner_vib_ZIP_file>\<partner_vib_ZIP_file>`

Las opciones para los comandos `update` e `install` permiten realizar un simulacro, especificar un VIB y omitir la comprobación del nivel de aceptación, entre otras acciones. No omita la comprobación en los sistemas de producción. Consulte la *Referencia de ESXCLI*.

4 Compruebe que los VIB estén instalados en el host ESXi.

```
esxcli --server=<server_name> software vib list
```

Actualizar un host con perfiles de imagen

Puede actualizar un host con perfiles de imagen almacenados en un almacén de software al que se puede acceder a través de una URL o en un almacén ZIP sin conexión.

Puede utilizar el comando `esxcli software profile update` o `esxcli software profile install` para actualizar un host ESXi.

Cuando actualiza un host, los comandos **`esxcli software profile update`** o **`esxcli software profile install`** aplican una versión posterior (principal o secundaria) de un perfil de imagen completo en el host. Después de finalizar esta operación y reiniciar, el host puede unirse a un entorno de vCenter Server de la misma versión o de una versión posterior.

El comando `esxcli software profile update` lleva los contenidos completos de la imagen de host ESXi al mismo nivel que el método de actualización correspondiente mediante un instalador ISO. Sin embargo, el instalador ISO realiza una comprobación previa a la actualización para detectar problemas potenciales, como memoria insuficiente o dispositivos no compatibles. El método de actualización **`esxcli`** solo realiza estas comprobaciones durante una actualización de ESXi 6.7 Update 1 o posterior a una versión más reciente.

Nota No utilice la opción `--dry-run` para las actualizaciones de ESXi 6.7.x y ESXi 7.0.x anteriores a 7.0 Update 3i a ESXi 8.0 y versiones posteriores. Cuando se elimina la opción `--dry-run`, puede seguir utilizando el método de actualización esxcli para actualizar de ESXi 6.7 Update 1 o posterior a ESXi 8.0 o posterior. En versiones anteriores a ESXi 6.7 Update 1, primero debe actualizar a 6.7 Update 1 o una versión posterior antes de actualizar a ESXi 8.0 o una versión posterior.

Para obtener más información sobre los métodos y el proceso de actualización de ESXi, consulte Descripción general del proceso de actualización del host ESXi.

Importante Si planea actualizar ESXi desde un paquete zip en un almacén suministrado por VMware, ya sea en línea desde el sitio web de VMware o descargado localmente, VMware admite solo el comando de actualización `esxcli software profile update --depot=<depot_location> --profile=<profile_name>`.

Cuando se especifica un servidor de destino mediante `--server=<server_name>`, el servidor le solicita un nombre de usuario y una contraseña. Se admiten otras opciones de conexión, como un archivo de configuración o un archivo de sesión. Para obtener una lista de opciones de conexión, consulte Introducción a ESXCLI o ejecute `esxcli --help` en el símbolo del sistema de ESXCLI.

Nota Las opciones de los comandos `update` y `install` permiten realizar un simulacro, omitir la comprobación de nivel de aceptación, ignorar las advertencias de comprobación de compatibilidad de hardware, etc. La opción para omitir las advertencias de comprobación de compatibilidad de hardware solo está disponible para ESXi 6.7 Update 1 o posterior. No omita la comprobación en los sistemas de producción.

Para obtener ayuda con las opciones, escriba `esxcli software profile install --help` o `esxcli software profile update --help`. Para obtener una lista completa de las opciones de línea de comandos disponibles, consulte Referencia de ESXCLI.

Requisitos previos

- Instale una instancia de ESXCLI independiente. Consulte *Introducción a ESXCLI*. Para solucionar problemas, ejecute comandos `esxcli` en ESXi Shell.
- Determine si una actualización requiere que el host se encuentre en el modo de mantenimiento o se reinicie. De ser necesario, coloque al host en el modo de mantenimiento.

Consulte Ver si la actualización de host ESXi requiere el modo de mantenimiento o el reinicio. Consulte Poner un host en modo de mantenimiento.

Importante Cuando utilice ESXCLI para actualizar el host, ponga el host en modo de mantenimiento de forma manual para asegurarse de que el disco de arranque no esté activamente en uso antes de que comience la actualización.

- Si la actualización requiere un reinicio y si el host pertenece a un clúster de vSphere HA, quite el host del clúster o desactive HA en el clúster.

Procedimiento

1 Determine qué VIB están instalados en el host.

```
esxcli --server=<server_name> software vib list
```

2 Determine qué perfiles de imagen hay disponibles en el almacén.

```
esxcli --server=<server_name> software sources profile list --depot=http://<web_server>/
<depot_name>
```

Puede especificar un servidor proxy mediante la opción `--proxy`.

3 Actualice el perfil de imagen existente para incluir los VIB o instalar nuevos VIB.

Importante El comando `software profile update` actualiza VIB existentes con los VIB correspondientes del perfil especificado, pero no afecta a otros VIB instalados en el servidor de destino. El comando `software profile install` instala los VIB presentes en el perfil de imagen del almacén y quita cualquier otro VIB instalado en el servidor de destino.

Opción	Descripción
Actualizar el perfil de imagen desde un paquete zip suministrado por VMware, en un almacén, al que se puede acceder en línea desde el sitio web de VMware o que se puede descargar en un almacén local	`esxcli software profile update --depot=<depot_location> --profile=<profile_name>` **Importante** Este es el único método de actualización que admite VMware para paquetes zip suministrados por VMware. Los nombres de paquetes zip suministrados por VMware tienen este formato: `VMware-ESXi-<version_number>-<build_number>-depot.zip`. El nombre del perfil para paquetes zip suministrados por VMware tiene uno de los siguientes formatos. ■ `ESXi-<version_number>-<build_number>-standard` ■ `ESXi-<version_number>-<build_number>-notools` (no incluye VMware Tools)
Actualizar el perfil de imagen desde un almacén accesible mediante URL	`esxcli --server=<server_name> software profile update --depot=http://<web_server>/<depot_name> --profile=<profile_name>`

Opción	Descripción
Actualizar el perfil de imagen desde el archivo ZIP almacenado de forma local en el servidor de destino	`esxcli --server=<server_name> software profile update --depot=file:///<path_to_profile_ZIP_file>/<profile_ZIP_file> --profile=<profile_name>`
Actualizar el perfil de imagen desde un archivo ZIP en el servidor de destino, copiado en un almacén de datos	`esxcli --server=<server_name> software profile update --depot=<datastore_name>/<profile_ZIP_file> --profile=<profile_name>`
Actualizar el perfil de imagen desde un archivo ZIP copiado de forma local y aplicado en el servidor de destino	`esxcli --server=<server_name> software profile update --depot=/<root_dir>/<path_to_profile_ZIP_file>/<profile_ZIP_file> --profile=<profile_name>`
Instalar todos los VIB nuevos en un perfil especificado accesible mediante URL	`esxcli --server=<server_name> software profile install --depot=http://<web_server>/<depot_name> --profile=<profile_name>`
Instalar todos los VIB nuevos en un perfil especificado desde un archivo ZIP almacenado de forma local en el destino	`esxcli --server=<server_name> software profile install --depot=file:///<path_to_profile_ZIP_file>/<profile_ZIP_file> --profile=<profile_name>`
Instalar todos los VIB nuevos desde un archivo ZIP en el servidor de destino, copiado en un almacén de datos	`esxcli --server=<server_name> software profile install --depot=<datastore_name>/<profile_ZIP_file> --profile=<profile_name>`
Instalar todos los VIB nuevos desde un archivo ZIP copiado de forma local y aplicado en el servidor de destino	`esxcli --server=<server_name> software profile install --depot=/<root_dir>/<path_to_profile_ZIP_file>/<profile_ZIP_file> --profile=<profile_name>`

4 Compruebe que los VIB estén instalados en el host ESXi.

```
esxcli --server=<server_name> software vib list
```

Actualizar hosts ESXi mediante archivos .zip

Puede actualizar hosts con perfiles de imagen o VIB descargando un archivo ZIP de un almacén.

Los socios de VMware preparan VIB de otros fabricantes para proporcionar agentes de administración o controladores lanzados de manera asíncrona.

Importante Si va a actualizar ESXi desde un paquete zip en un almacén suministrado por VMware, ya sea en línea en el sitio web de VMware o descargado de forma local, los comandos `esxcli software vib update` y `esxcli software vib install` no son compatibles. VMware solo admite los métodos de actualización especificados para los almacenes proporcionados por VMware en el tema Actualizar un host con perfiles de imagen . Si el almacén no lo proporciona VMware y no tiene un perfil de imagen, puede utilizar los comandos `esxcli software vib update` y `esxcli software vib install` para las actualizaciones de VIB individuales o múltiples, como se describe en Actualizar un host con VIB individuales y el procedimiento de este tema.

Cuando se especifica un servidor de destino mediante --server=<*server_name*>, el servidor le solicita un nombre de usuario y una contraseña. Se admiten otras opciones de conexión, como un archivo de configuración o un archivo de sesión. Para obtener una lista de opciones de conexión, consulte Introducción a ESXCLI o ejecute `esxcli --help` en el símbolo del sistema de ESXCLI.

Requisitos previos

- Instale ESXCLI. Consulte Introducción a ESXCLI. Para solucionar problemas, ejecute comandos `esxcli` en ESXi Shell.
- Descargue el archivo ZIP de un paquete de almacén de un partner externo de VMware.
- Determine si una actualización requiere que el host se encuentre en el modo de mantenimiento o se reinicie. De ser necesario, coloque al host en el modo de mantenimiento.

  Consulte Ver si la actualización de host ESXi requiere el modo de mantenimiento o el reinicio. Consulte Poner un host en modo de mantenimiento.
- Si la actualización requiere un reinicio y si el host pertenece a un clúster de vSphere HA, quite el host del clúster o desactive HA en el clúster.

Procedimiento

◆ Instale el archivo ZIP.

```
esxcli --server=<server_name> software vib update --depot=/<path_to_vib_ZIP>/
<ZIP_file_name>.zip
```

Quitar VIB de un host

Puede desinstalar los VIB de terceros o los VIB de VMware del host ESXi, a menos que el VIB forme parte de un componente que sea necesario para el ciclo de vida de ESXi o un controlador.

Los socios de VMware preparan VIB de otros fabricantes para proporcionar agentes de administración o controladores lanzados de manera asíncrona.

Importante A partir de ESXi 8.0 Update 2, la eliminación de algunos VIB de sus componentes puede generar problemas de tiempo de ejecución con ESXi.

Tabla 3-11. VIB necesarios para la finalización de la imagen ESXi.

Componente	VIB
ESXi	bmcal
	bmcal-esxio
	clusterstore
	cpu-microcode
	crx
	drivervm-gpu
	esx-base
	esx-dvfilter-generic-fastpath
	esx-ui
	esx-xserver
	esxio
	esxio-base
	esxio-combiner
	esxio-combiner-esxio
	esxio-dvfilter-generic-fastpath
	gc
	gc-esxio
	native-misc-drivers
	infravisor
	native-misc-drivers-esxio
	pensandoatlas
	trx
	vdfs
	vsan
	vsanhealth
esx-update	esx-update
	loadesx
esxio-update	esxio-update
	loadesxio
Intel-ne1000	ne1000

Instale ESXCLI. Consulte Introducción a ESXCLI. Para solucionar problemas, ejecute comandos `esxcli` en ESXi Shell.

Requisitos previos

- Si la eliminación requiere un reinicio y si el host pertenece a un clúster de vSphere HA, desactive HA para el host.
- Determine si una actualización requiere que el host se encuentre en el modo de mantenimiento o se reinicie. De ser necesario, coloque al host en el modo de mantenimiento.

  Consulte Ver si la actualización de host ESXi requiere el modo de mantenimiento o el reinicio. Consulte Poner un host en modo de mantenimiento.

  Nota Para asegurarse de que el disco de arranque no esté activamente en uso al utilizar ESXCLI para actualizar el host, póngalo manualmente en el modo de mantenimiento.
- Instale ESXCLI. Consulte Introducción a ESXCLI. Para solucionar problemas, ejecute comandos `esxcli` en ESXi Shell.

Procedimiento

1 Apague cada máquina virtual que se ejecuta en el host ESXi.

Nota Puede enumerar todas las máquinas virtuales en ejecución y recuperar el identificador de ámbito de cada una ejecutando el siguiente comando.

```
esxcli --server=<server_name> vm process list
```

Opción	Comando
Para desactivar el sistema operativo invitado y luego apagar la máquina virtual	`esxcli --server=<server_name> vm process kill --type soft --world-id <vm_ID>`
Para apagar inmediatamente la máquina virtual	`esxcli --server=<server_name> vm process kill --type hard --world-id <vm_ID>`
Para forzar la operación de apagado	`esxcli --server=<server_name> vm process kill --type force --world-id <vm_ID>`

Como alternativa, para evitar apagar las máquinas virtuales, se las puede migrar a otro host. Consulte el tema Migrar máquinas virtuales en la documentación de *Administrar vCenter Server y hosts*.

2 Coloque el host en modo de mantenimiento.

```
esxcli --server=<server_name> system maintenanceMode set --enable true
```

3 Si es necesario, apague o migre las máquinas virtuales.

4 Determine qué VIB están instalados en el host.

```
esxcli --server=<server_name> software vib list
```

5 Elimine el VIB.

```
esxcli --server=<server_name> software vib remove --vibname=<name>
```

Especifique uno o más VIB para eliminarlos de una de las siguientes maneras.

- *<name>*
- *<name>*:*<version>*
- *<vendor>*:*<name>*
- *<vendor>*:*<name>*:*<version>*

Por ejemplo, el comando para eliminar un VIB especificado por proveedor, nombre y versión puede tener el siguiente formato.

```
esxcli --server myEsxiHost software vib remove --vibname=PatchVendor:patch42:version3
```

Nota El comando `remove` admite varias opciones más. Consulte *Referencia de ESXCLI*.

Agregar extensiones de terceros a hosts con un comando ESXCLI

Puede utilizar el comando `esxcli software vib` para agregar al sistema una extensión de terceros lanzada como paquete de VIB.

Al utilizar este comando, el sistema VIB actualiza el conjunto de reglas de firewall y el daemon para el host después de que se reinicia el sistema.

De lo contrario, puede utilizar un archivo de configuración de firewall para especificar las reglas de puerto de los servicios de host donde desea permitir la extensión. En la documentación de *Seguridad de vSphere* se explica la forma de agregar, aplicar y actualizar un conjunto de reglas de firewall, y se enumeran los comandos `esxcli network firewall`.

Realizar un simulacro de una instalación o actualización de ESXCLI

Puede utilizar la opción `--dry-run` para obtener una vista previa de los resultados de una operación de instalación o actualización.

Cuando se especifica un servidor de destino mediante `--server=<server_name>`, el servidor le solicita un nombre de usuario y una contraseña. Se admiten otras opciones de conexión, como un archivo de configuración o un archivo de sesión. Para obtener una lista de opciones de conexión, consulte Introducción a ESXCLI o ejecute `esxcli --help` en el símbolo del sistema de ESXCLI.

Requisitos previos

El simulacro de un procedimiento de instalación o actualización no realiza ningún cambio, pero informa sobre las operaciones a nivel de VIB que se realizarían si ejecuta el comando sin la opción `--dry-run`.

Instale ESXCLI. Consulte Introducción a ESXCLI. Para solucionar problemas, ejecute comandos `esxcli` en ESXi Shell.

Procedimiento

1 Introduzca el comando de instalación o actualización con la opción `--dry-run`.

- ```
  esxcli --server=<server_name> software vib install --dry-run
  ```
- ```
  esxcli --server=<server_name> software vib update --dry-run
  ```
- ```
  esxcli --server=<server_name> software profile install --dry-run
  ```
- ```
  esxcli --server=<server_name> software profile update --dry-run
  ```

2 Revise el resultado que se devuelve.

   El resultado muestra qué VIB se van a instalar o eliminar e indica si la instalación o actualización requiere un reinicio.

Enumerar los VIB y los perfiles disponibles después del reinicio del host

Puede usar la opción `--rebooting-image` para enumerar los VIB y perfiles que están instalados en el host y que estarán activos después del siguiente reinicio del host.

Cuando se especifica un servidor de destino mediante `--server=<server_name>`, el servidor le solicita un nombre de usuario y una contraseña. Se admiten otras opciones de conexión, como un archivo de configuración o un archivo de sesión. Para obtener una lista de opciones de conexión, consulte Introducción a ESXCLI o ejecute `esxcli  --help` en el símbolo del sistema de ESXCLI.

Requisitos previos

Instale ESXCLI. Consulte Introducción a ESXCLI. Para solucionar problemas, ejecute comandos `esxcli` en ESXi Shell.

Procedimiento

1 Ingrese uno de los siguientes comandos.

Opción	Descripción
Para VIB	`esxcli --server=<server_name> software vib list --rebooting-image`
Para perfiles	`esxcli --server=<server_name> software profile get --rebooting-image`

2 Revise el resultado que se devuelve.

El resultado muestra información para la imagen de ESXi que se activará después del siguiente reinicio. Si no se ha creado la imagen de reinicio pendiente, la salida no arroja nada.

Mostrar el perfil de imagen y el nivel de aceptación del host

Puede utilizar el comando `software profile get` para visualizar el perfil de imagen actualmente instalado y el nivel de aceptación del host especificado.

Este comando también muestra detalles del historial de perfiles de imagen instalados, incluidas las modificaciones a los perfiles.

Cuando se especifica un servidor de destino mediante `--server=<server_name>`, el servidor le solicita un nombre de usuario y una contraseña. Se admiten otras opciones de conexión, como un archivo de configuración o un archivo de sesión. Para obtener una lista de opciones de conexión, consulte Introducción a ESXCLI o ejecute `esxcli --help` en el símbolo del sistema de ESXCLI.

Requisitos previos

Instale ESXCLI. Consulte Introducción a ESXCLI. Para solucionar problemas, ejecute comandos `esxcli` en ESXi Shell.

Procedimiento

1 Introduzca el siguiente comando.

```
esxcli --server=<nombre_del_servidor> software profile get
```

2 Examine el resultado.

Después de actualizar hosts ESXi

Para completar una actualización del host, asegúrese de que el host se reconecte a su vCenter Server de administración y se reconfigure en caso de que sea necesario. También puede comprobar que el host posea las licencias correctas.

Después de actualizar un host ESXi, realice las siguientes acciones:

- Consulte los registros de actualización. Puede utilizar vSphere Client para exportar los archivos de registro.
- Si un sistema vCenter Server administra el host, deberá reconectar el host a vCenter Server haciendo clic con el botón derecho en el inventario de vCenter Server y seleccionando **Conectar**.
- Cuando se complete la actualización, el host ESXi se encuentra en el modo de evaluación. El período de evaluación tiene una duración de 60 días. Deberá asignar una licencia de vSphere 8.0 antes de que venza el período de evaluación. Puede actualizar las licencias existentes o adquirir nuevas desde My VMware. Utilice vSphere Client para configurar las licencias para el host de su entorno. Consulte la documentación *Administración de hosts y vCenter Server* para obtener información sobre la administración de licencias en vSphere.
- Es posible que sea necesario volver a numerar los dispositivos sdX del host después de la actualización. De ser necesario, actualice cualquier script que haga referencia a los dispositivos sdX.
- Actualice las máquinas virtuales en el host. Consulte Actualizar máquinas virtuales y VMware Tools.
- Configure el servicio vSphere Authentication Proxy. Las versiones anteriores de vSphere Authentication Proxy no son compatibles con vSphere 8.0. Consulte la documentación de *vSphere Security* para obtener detalles sobre la configuración del servicio vSphere Authentication Proxy.

Acerca de los modos de evaluación y con licencia de ESXi

Puede utilizar el modo de evaluación para explorar un conjunto de características igual a la licencia de vSphere Enterprise Plus.

Puede utilizar el modo de evaluación para explorar el conjunto completo de funciones para los hosts ESXi. El modo de evaluación proporciona un conjunto de funciones equivalente a una licencia de vSphere Enterprise Plus. Antes de que finalice el modo de evaluación, debe asignar a sus hosts una licencia que admita todas las funciones en uso. Por ejemplo, en el modo de evaluación, puede utilizar la tecnología vSphere vMotion, la función vSphere HA, la característica vSphere DRS y otras características. Si desea continuar utilizando estas funciones, debe asignar una licencia que las admita.

La versión de los hosts ESXi Installable se instala siempre en el modo de evaluación. ESXi Embedded se ofrece preinstalado en el dispositivo de almacenamiento interno por parte de cada proveedor de hardware. Podría estar en el modo de evaluación o con licencia previa.

El período de evaluación es de 60 días y comienza cuando se enciende el host ESXi. En cualquier momento durante el período de evaluación de 60 días, se puede realizar la conversión de un modo con licencia a un modo de evaluación. El tiempo disponible en el modo de evaluación se resta del tiempo ya consumido.

Por ejemplo, supongamos que se utiliza un host ESXi en el modo de evaluación durante 20 días y, a continuación, se asigna una clave de licencia de vSphere Standard Edition al host. Si se vuelve a establecer el host en el modo de evaluación, se podrá explorar el conjunto completo de funciones para el host durante el período de evaluación restante de 40 días.

Cuando expira el período de evaluación o la licencia de los hosts ESXi, estos se desconectan de vCenter Server. Todas las máquinas virtuales que estén encendidas continúan funcionando, pero no puede encender las máquinas virtuales una vez que se apagan. No puede cambiar la configuración actual de las características que están en uso. No se pueden utilizar las características que permanecieron sin usar antes de la caducidad de la licencia.

Para obtener información sobre la administración de licencias para los hosts ESXi, consulte la documentación *Administrar vCenter Server y hosts*.

Licencias para hosts ESXi tras la actualización

Después de actualizar a ESXi 8.0, debe aplicar una licencia de vSphere 8.

Si actualiza un host ESXi a una versión que comienza con el mismo número, no es necesario que reemplace la licencia existente por una nueva. Por ejemplo, si actualiza un host de la versión ESXi 6.5 a 6.7, puede usar la misma licencia para el host.

Si actualiza un host ESXi a una versión que comienza con un número distinto, debe aplicar una nueva licencia. Por ejemplo, si actualiza un host ESXi de 7.x a 8.0, debe concederle al host una licencia de vSphere 8.

Cuando se actualizan hosts ESXi 6.7 o ESXi 7.0 a ESXi 8.0, los hosts entran en un modo de evaluación por un período de 60 días hasta que se aplican las licencias correspondientes para vSphere 8. Consulte Acerca de los modos de evaluación y con licencia de ESXi.

Puede adquirir licencias de vSphere 8 desde My VMware. Una vez que tenga las licencias de vSphere 8, deberá asignarlas a todos los hosts ESXi 8.0 actualizados mediante la funcionalidad de administración de licencias en vSphere Client. Consulte la documentación de *Administrar vCenter Server y hosts* para obtener detalles. Si usa el método generado por script para la actualización a ESXi 8.0, puede proporcionar la clave de licencia en el archivo kickstart (ks).

Ejecutar el script de validación de arranque seguro después de la actualización de ESXi

Después de actualizar un host ESXi desde una versión que no admite el arranque seguro UEFI, debe comprobar si puede activar el arranque seguro.

Para que el arranque seguro se realice correctamente, la firma de cada VIB instalado debe estar disponible en el sistema. Las versiones anteriores de ESXi no guardan las firmas cuando se instalan los VIB.

- Si realiza la actualización mediante comandos ESXCLI, la versión anterior de ESXi instalará los nuevos VIB, por lo que no se guardarán las firmas y no será posible realizar el arranque seguro.

- Si realiza la actualización mediante el archivo ISO, se guardarán las firmas de los nuevos VIB. Esto también es así para las actualizaciones de vSphere Lifecycle Manager que utilicen el archivo ISO.
- Si los VIB anteriores permanecen en el sistema, las firmas de dichos VIB no estarán disponibles y no será posible realizar el arranque seguro.
  - Si el sistema utiliza un controlador de terceros y la actualización de VMware no incluye una nueva versión del VIB de controlador, el VIB anterior permanecerá en el sistema tras la actualización.
  - En casos excepcionales, VMware puede descartar el desarrollo en curso de un VIB específico sin proporcionar un nuevo VIB que lo reemplace o lo deje obsoleto, de manera que el VIB anterior permanece en el sistema tras la actualización.

Nota El arranque seguro UEFI también requiere un cargador de arranque actualizado. Este script no comprueba que haya un cargador de arranque actualizado.

Requisitos previos

Después de actualizar un host ESXi a partir de una versión anterior de ESXi que no admitía el arranque seguro UEFI, es posible que pueda activar el arranque seguro. La posibilidad de activar el arranque seguro depende de la forma en la que se haya hecho la actualización y de si esta reemplazó todos los VIB existentes o dejó alguno sin modificar. Puede ejecutar el script de validación después de realizar la actualización para determinar si la instalación actualizada admite el arranque seguro.

- Verifique que el hardware admita el arranque seguro UEFI.
- Verifique que todos los VIB estén firmados con un nivel de aceptación PartnerSupported, como mínimo. Si incluye VIB en el nivel CommunitySupported, no podrá usar el arranque seguro.

Procedimiento

1 Actualice ESXi y ejecute el siguiente comando.

```
/usr/lib/vmware/secureboot/bin/secureBoot.py -c
```

2 Compruebe el resultado.

El resultado incluye `Secure boot can be enabled` o `Secure boot CANNOT be enabled`.

Configurar Syslog en hosts ESXi

Puede utilizar vSphere Client, VMware Host Client o el comando `esxcli system syslog` para configurar el servicio syslog.

El servicio Syslog recibe, clasifica y almacena mensajes de registro para análisis que le ayudarán a tomar medidas preventivas en su entorno.

Establezca Syslog de ESXi mediante vSphere Client

Puede usar el comando vSphere Client para configurar el servicio Syslog de forma global y editar varias opciones avanzadas.

Procedimiento

1 Desplácese hasta el host ESXi en el inventario de vSphere Client.

2 Haga clic en **Configurar**.

3 En **Sistema**, haga clic en **Configuración avanzada del sistema**.

4 Haga clic en **Editar**.

5 Filtre por **`syslog`**.

6 Para configurar globalmente el registro y configurar varias opciones avanzadas, consulte Opciones de Syslog de ESXi.

7 (opcional) Para sobrescribir los valores predeterminados de tamaño de registro y rotación de registros de cualquier registro:

   a Haga clic en el nombre del registro que desea personalizar.

   b Introduzca el número de rotaciones y el tamaño de registro que desea.

8 Haga clic en **Aceptar**.

Resultados

Los cambios en las opciones de syslog surten efecto.

Nota La configuración de parámetros de Syslog que se define mediante vSphere Client o VMware Host Client se aplica inmediatamente. Sin embargo, la mayoría de los ajustes que se definen mediante ESXCLI requieren un comando adicional para que surtan efecto. Para obtener más información, consulte Opciones de Syslog de ESXi.

Establezca Syslog de ESXi mediante VMware Host Client

Puede utilizar VMware Host Client para configurar y editar parámetros de servicio de Syslog en hosts ESXi.

Procedimiento

1 En VMware Host Client, en **Host**, haga clic en **Administrar** > **Sistema** > **Configuración avanzada**.

2 En el panel **Buscar**, escriba una configuración de Syslog que desee definir. Consulte Opciones de Syslog de ESXi.

3 Seleccione la opción y haga clic en **Editar opción**.

4 Establezca el valor como se describe en la tabla de parámetros de Opciones de Syslog de ESXi.

5 Haga clic en **Guardar**.

Establecer Syslog ESXi mediante ESXCLI

Puede configurar el servicio Syslog en hosts ESXi mediante el comando ESXCLI: `esxcli system syslog config set <syslog option>`.

Requisitos previos

Para obtener información sobre el uso del comando esxcli system syslog y otros comandos de ESXCLI, consulte Introducción a ESXCLI. Para obtener más información sobre cómo abrir el firewall de ESXi para el puerto definido en cada especificación de host remoto, consulte Configurar el firewall de ESXi.

Nota El uso de ESXCLI requiere que ESXi abra los inicios de sesión SSH, lo cual supone un riesgo de seguridad y no se recomienda. Si decidió utilizar ESXCLI, asegúrese de utilizar el comando `esxcli system syslog reload` después de configurar cada parámetro para asegurarse de que se aplique.

Procedimiento

- Utilice el comando ESXCLI `esxcli system syslog config set <syslog option>` para establecer una opción de Syslog que decida habilitar. Por ejemplo, para establecer la opción `Syslog.global.logHost`, utilice el comando `esxcli system syslog config set --loghost=<str>`

  Después de configurar `Syslog.global.logHost`, los hosts ESXi abren y mantienen las conexiones con los recopiladores de Syslog, y la transmisión de mensajes comienza inmediatamente. Cuando ESXi genera un mensaje de Syslog, lo escribe en el archivo de registro adecuado en el host ESXi y también lo reenvía a todos los recopiladores de Syslog configurados.

Opciones de Syslog de ESXi

Puede definir el comportamiento de las transmisiones y los archivos de syslog de ESXi mediante un conjunto de opciones de syslog.

Además de la configuración básica, como Syslog.global.logHost, a partir de ESXi 7.0 Update 1, hay disponible una lista de opciones avanzadas para las personalizaciones y el cumplimiento de NIAP.

Nota Configure siempre el almacenamiento persistente antes de establecer alguno de los parámetros de registro de auditoría o el parámetro de Syslog.global.logDir.

Nota Todos los ajustes del registro de auditoría que comienzan por Syslog.global.auditRecord se aplican inmediatamente. Sin embargo, para otros ajustes que defina mediante ESXCLI, asegúrese de ejecutar el comando esxcli system syslog reload para habilitar los cambios.

Tabla 3-12. Opciones de Syslog heredadas

Opción	Comando ESXCLI	Descripción
Syslog.global.logHost	esxcli system syslog config set --loghost=<str>	Define una lista delimitada por comas de hosts remotos y especificaciones para transmisiones de mensajes. Si el campo loghost=<str> está en blanco, no se reenvía ningún registro. Si bien no existe un límite estricto para la cantidad de hosts remotos que recibirán mensajes de Syslog, una buena práctica es mantener el número de hosts remotos en cinco o menos. El formato de una especificación de host remoto es: protocol://hostname|ipv4|'['ipv6']'[:port]. El protocolo debe ser TCP, UDP o SSL. El valor de los puertos puede ser cualquier número decimal entre 1 y 65535. Si no se proporciona un puerto, SSL y TCP utilizan 1514. UDP utiliza 514. Por ejemplo: ssl://hostName1:1514.
Syslog.global.defaultRotate	esxcli system syslog config set --default-rotate=<long>	Número máximo de archivos de registro antiguos que se conservarán. Puede configurar este número en forma global y para subregistradores individuales (consulte Syslog.global.defaultSize).
Syslog.global.defaultSize	esxcli system syslog config set --default-size=<long>	Tamaño predeterminado de los archivos de registro, en KiB. Una vez que un archivo alcanza el tamaño predeterminado, el servicio de Syslog crea un nuevo archivo. Puede configurar este número en forma global y para subregistradores individuales.

Tabla 3-12. Opciones de Syslog heredadas (continuación)

Opción	Comando ESXCLI	Descripción
Syslog.global.logDir	esxcli system syslog config set --logdir=<str>	Directorio donde residen los registros. El directorio puede encontrarse en volúmenes NFS o VMFS montados. Solo el directorio /scratch del sistema de archivos local se mantiene en todos los reinicios. Especifique el directorio como [*nombrealmacéndatos*] *ruta_a_archivo*, donde la ruta de acceso es relativa a la raíz del volumen que respalda el almacén de datos. Por ejemplo, la ruta de acceso [storage1] /systemlogs se asigna a la ruta de acceso /vmfs/volumes/storage1/systemlogs.
Syslog.global.logDirUnique	esxcli system syslog config set --logdir-unique=<bool>	Especifica el nombre de host ESXi que se va a concatenar al valor de Syslog.global.logDir. Es fundamental que habilite esta opción cuando varios hosts ESXi inicien sesión en un sistema de archivos compartido. Al seleccionar esta opción, se crea un subdirectorio con el nombre del host ESXi del directorio especificado por **Syslog.global.LogDir**. Un directorio único es útil si varios hosts ESXi utilizan el mismo directorio NFS.
Syslog.global.certificate.checkSSLCerts	esxcli system syslog config set --check-ssl-certs=<bool>	Examine la comprobación de certificados SSL al transmitir mensajes a hosts remotos.

Tabla 3-13. Opciones de Syslog disponibles a partir de ESXi 7.0 Update 1

Opción	Comando ESXCLI	Descripción
Syslog.global.auditRecord.storageCapacity	esxcli system auditrecords local set --size=<long>	Especifica la capacidad del directorio de almacenamiento de registros de auditoría ubicado en el host ESXi, en MiB. No se puede reducir la capacidad del almacenamiento de registros de auditoría. Puede aumentar la capacidad antes o después de habilitar el almacenamiento de registros de auditoría (consulte Syslog.global.auditRecord.storageEnable).

Tabla 3-13. Opciones de Syslog disponibles a partir de ESXi 7.0 Update 1 (continuación)

Opción	Comando ESXCLI	Descripción
`Syslog.global.auditRecord.remoteEnable`	`esxcli system auditrecords remote enable`	Habilita el envío de registros de auditoría a hosts remotos. Los hosts remotos se especifican mediante el parámetro `Syslog.global.logHost`.
`Syslog.global.auditRecord.storageDirectory`	`esxcli system auditrecords local set --directory=<dir>`	Crea un directorio de almacenamiento de registros de auditoría y, a menos que se especifique, establece `/scratch/auditLog` como la ubicación predeterminada. No debe crear manualmente un directorio de almacenamiento de registros de auditoría y no puede cambiar el directorio de almacenamiento de registros de auditoría mientras esté habilitado el almacenamiento de registros de auditoría (consulte `Syslog.global.auditRecord.storageEnable`).
`Syslog.global.auditRecord.storageEnable`	`esxcli system auditrecords local enable`	Habilita el almacenamiento de registros de auditoría en un host ESXi. Si el directorio de almacenamiento de registros de auditoría no existe, se crea con la capacidad especificada por `Syslog.global.auditRecord.storageCapacity`.
`Syslog.global.certificate.checkCRL`	`esxcli system syslog config set --crl-check=<bool>`	Habilita la comprobación del estado de revocación de todos los certificados de una cadena de certificados SSL. Habilita la verificación de las CRL X.509 que no se comprueban de forma predeterminada en cumplimiento de las convenciones del sector. Una configuración validada por NIAP requiere comprobaciones de CRL. Debido a las limitaciones de implementación, si se habilitan las comprobaciones de CRL, todos los certificados de una cadena de certificados deben proporcionar un vínculo de CRL. No habilite la opción `crl-check` para instalaciones no relacionadas con la certificación, debido a la dificultad de configurar correctamente un entorno que utilice comprobaciones de CRL.

Tabla 3-13. Opciones de Syslog disponibles a partir de ESXi 7.0 Update 1 (continuación)

Opción	Comando ESXCLI	Descripción
`Syslog.global.certificate.strictX509Compliance`	`esxcli system syslog config set --x509-strict=<bool>`	Habilita la conformidad estricta con X.509. Realiza comprobaciones de validez adicionales en los certificados raíz de CA durante la verificación. Por lo general, estas comprobaciones no se realizan, ya que las raíces de CA son de confianza inherente y podrían producir incompatibilidades con las raíces de CA existentes y mal configuradas. Una configuración validada por NIAP requiere que incluso las raíces de CA pasen las validaciones. No habilite la opción `x509-strict` para instalaciones no relacionadas con la certificación, debido a la dificultad de configurar correctamente un entorno que utilice comprobaciones de CRL.
`Syslog.global.droppedMsgs.fileRotate`	`esxcli system syslog config set --drop-log-rotate=<long>`	Especifica el número de archivos antiguos de registro de mensajes descartados que se conservarán.
`Syslog.global.droppedMsgs.fileSize`	`esxcli system syslog config set --drop-log-size=<long>`	Especifica el tamaño de cada archivo de registro de mensajes descartados antes de cambiar a uno nuevo, en KiB.
`Syslog.global.logCheckSSLCerts`	`esxcli system syslog config set --check-ssl-certs=<bool>`	Examine la comprobación de certificados SSL al transmitir mensajes a hosts remotos. **Nota** Obsoleto. Use `Syslog.global.certificate.checkSSLCerts` en ESXi 7.0 Update 1 y posterior.

Tabla 3-13. Opciones de Syslog disponibles a partir de ESXi 7.0 Update 1 (continuación)

<table>
<tr><th>Opción</th><th>Comando ESXCLI</th><th>Descripción</th></tr>
<tr><td>Syslog.global.logFilters</td><td>esxcli system syslog config logfilter [add | remove | set] ...</td><td>Especifica una o varias especificaciones de filtrado de registros. Cada filtro de registro debe estar separado por una barra vertical doble (||). El formato de los filtros de registro es: numLogs | ident | logRegexp. numLogs establece la cantidad máxima de entradas de registro para los mensajes de registro especificados. Una vez alcanzado este número, se filtran y se omiten los mensajes de registro especificados. ident especifica uno o más componentes del sistema para aplicar el filtro a los mensajes de registro que generan estos componentes. logRegexp especifica una frase que distingue mayúsculas de minúsculas con la sintaxis de la expresión regular Python para filtrar los mensajes de registro según su contenido.</td></tr>
<tr><td>Syslog.global.logFiltersEnable</td><td></td><td>Habilita el uso de filtros de registro.</td></tr>
<tr><td>Syslog.global.logLevel</td><td>esxcli system syslog config set --log-level=<str></td><td>Especifica el nivel de filtrado de registros. Debe cambiar este parámetro solo para solucionar problemas relacionados con el daemon de syslog. Puede utilizar los valores debug para el nivel más detallado, info para el nivel de detalle predeterminado, warning solo para advertencias o errores, o error solo para errores.</td></tr>
<tr><td>Syslog.global.msgQueueDropMark</td><td>esxcli system syslog config --queue-drop-mark=<long>)</td><td>Especifica el porcentaje de la capacidad de la cola de mensajes a partir del cual se descartan los mensajes.</td></tr>
<tr><td>Syslog.global.remoteHost.connectRetryDelay</td><td>esxcli system syslog config set --default-timeout=<long></td><td>Especifica el retraso antes de volver a intentar conectarse a un host remoto después de que se haya producido un error en un intento de conexión, en segundos.</td></tr>
</table>

Tabla 3-13. Opciones de Syslog disponibles a partir de ESXi 7.0 Update 1 (continuación)

Opción	Comando ESXCLI	Descripción
`Syslog.global.remoteHost.maxMsgLen`	`esxcli system syslog config set --remote-host-max-msg-len=<long>`	Para los protocolos TCP y SSL, este parámetro especifica la longitud máxima de una transmisión de Syslog antes de que se produzca truncamiento, en bytes. La longitud máxima predeterminada para los mensajes de host remoto es 1 KiB. Puede aumentar la longitud máxima del mensaje hasta 16 KiB. No obstante, aumentar este valor por encima de 1 KiB no garantiza que las transmisiones largas lleguen sin truncar a un recopilador de Syslog. Por ejemplo, cuando la infraestructura de syslog que emite un mensaje es externa a ESXi. Esta configuración no afecta al protocolo UDP. RFC 5426 establece la longitud máxima de transmisión de mensajes para el protocolo UDP en 480 bytes para IPV4 y 1180 bytes para IPV6. Debido a esta restricción, y debido a que la infraestructura de redes puede descartar de forma arbitraria los paquetes UDP, no se recomienda el uso de UDP para transmitir mensajes críticos de Syslog.
`Syslog.global.vsanBacking`	`esxcli system syslog config set --vsan-backing=<bool>`	Permite que los archivos de registro y el directorio de almacenamiento de registros de auditoría se coloquen en un clúster de vSAN. Sin embargo, si se habilita este parámetro, es posible que el host ESXi deje de responder.

Ajustar syslog en hosts ESXi

Al utilizar la configuración de Syslog correcta, puede lograr una supervisión proactiva del entorno, reducir el tiempo de inactividad y tomar medidas preventivas en los servidores.

Al configurar syslog, debe tener en cuenta varios parámetros que afectan a la retención de archivos de registro, la transmisión de syslog, la longitud de la transmisión, el control de errores y la configuración de certificados SSL para la transmisión segura de mensajes de syslog. A continuación se muestran recomendaciones para ajustar los parámetros de syslog. Puede ver una descripción de todos los parámetros disponibles en Opciones de Syslog de ESXi.

Cómo especificar la retención de archivos de registro

De forma predeterminada, los archivos de registro no pueden expandirse más allá de un tamaño configurado. Una vez que un archivo de registro alcanza el tamaño configurado, el registro se enruta a un nuevo archivo de registro y se elimina el archivo de registro más antiguo.

Nota La práctica recomendada es equilibrar los ajustes de rotación y tamaño. Aumentar el ajuste de rotación garantiza que los archivos syslog se generen con la frecuencia suficiente para evitar daños o destrucción potenciales en los otros archivos de registro. Aumentar el ajuste de tamaño reduce el tiempo necesario para cambiar a otro archivo de registro. El ajuste de tamaño óptimo es un múltiplo de 1024 KiB.

Utilice el ajuste `Syslog.global.defaultSize` para especificar el tamaño máximo del archivo de registro en KiB y `Syslog.global.defaultRotate` para establecer el número máximo de archivos de registro antiguos que se deben conservar antes de rotar a un nuevo archivo de registro. Para cambiar los parámetros de retención de archivos de registro asociados a un programa específico, utilice `Syslog.loggers.<progName>.rotate` y `Syslog.loggers.<progName>.size settings`, donde `<progName>` es el nombre del programa cuyos parámetros desea ajustar.

Administrar la configuración que afecta al archivo de registro de la máquina virtual

Puede configurar algunas opciones que afectan al archivo de registro de la máquina virtual (`vmware.log`) en el archivo `vmx` o en el archivo `/etc/vmware/config`. Debe apagar una máquina virtual para editar el archivo `vmx` y las ediciones solo surtirán efecto en esa máquina virtual. Si utiliza el archivo `/etc/vmware/config`, debe agregar el prefijo *"vmx"* a la configuración, por ejemplo `vmx.log.keepOld = "20"`, y las modificaciones afectan a todas las máquinas virtuales del host ESXi.

Tabla 3-14. Opciones configurables para el archivo vmware.log

Parámetro	Descripción	Ejemplo	Notas
`logging`	Deshabilita el registro de todas las máquinas virtuales.	El valor predeterminado es `logging = "TRUE"`. Para deshabilitar el registro de máquinas virtuales: `logging = "FALSE"`	No utilice esta configuración, ya que, al deshabilitar el registro de máquinas virtuales, resulta extremadamente difícil o imposible obtener soporte para los problemas de la máquina virtual. Si necesita utilizar esta opción por algún motivo, solo puede colocarla en el archivo `vmx` de una máquina virtual.
`log.throttleBytesPerSec`	Controla cuándo se regula un archivo de registro. La regulación de archivos de registro se produce cuando las escrituras en el archivo `vmware.log` superan la velocidad especificada durante una cantidad significativa de tiempo. Esto ocurre cuando el código dentro del proceso VMX, el cual controla una máquina virtual, crea demasiados mensajes de registro. El valor predeterminado para esta opción es 1 KB/s. En el caso de que se regule el registro, verá `<<< Log Throttled >>>` en el archivo `vmware.log`.	`log.throttleBytesPerSec = "1500"` Para deshabilitar la regulación del registro, utilice `log.throttleBytesPerSec = "0xFFFFFFFF"`	La regulación del archivo de registro puede ocultar la información necesaria para diagnosticar problemas con la máquina virtual afectada. Si necesita deshabilitar la regulación de registros, coloque la línea del ejemplo en el archivo `vmx` de la máquina virtual afectada. Elimine la línea una vez que finalice la sesión de depuración.
`log.keepOld`	Controla el número de archivos `vmware.log` antiguos que se conservarán.	`log.keepOld = "20"`	No coloque el valor de esta opción por debajo del valor predeterminado (10). Si las máquinas virtuales se modifican o mueven con frecuencia, considere la posibilidad de aumentar esta opción a 20 o más.

Tabla 3-14. Opciones configurables para el archivo vmware.log (continuación)

Parámetro	Descripción	Ejemplo	Notas

`log.rotateSize`	Controla el tamaño máximo de un archivo `vmware.log` en bytes.	`log.rotateSize = "2500000"`
		Para deshabilitar la limitación del tamaño máximo de un archivo `vmware.log`, utilice
		`log.rotateSize = "0"`
			Un valor de esta opción inferior a 100.000 puede provocar la pérdida de mensajes de registro críticos y afectar al rendimiento de la máquina virtual. En ESXi 7.x y versiones anteriores, el valor predeterminado de esta opción no establece ningún límite en el tamaño de un archivo `vmware.log`. En ESXi 8.x y versiones posteriores, el valor predeterminado de esta opción es 2.048.000.

`log.fileName`	Controla el nombre y la ubicación de los archivos de registro de la máquina virtual.	`log.fileName = "myVMLog"`
		Esta opción cambia el nombre de los archivos de registro de la máquina virtual de vmware.log a `myVMlog`.
		`log.fileName = "/vmfs/volumes/vol1/myVM/myVM.log"`
		Esta opción dirige los archivos de registro de la máquina virtual a un directorio de un volumen de VMFS diferente (vol1) al utilizar `myVM` para un nombre de archivo.
			No coloque un archivo de registro fuera del directorio de la máquina virtual para asegurarse de que la recopilación de paquetes de soporte del host seleccione el archivo de registro, el cual puede ser determinante a la hora de depurar los problemas de la máquina virtual.

Tabla 3-14. Opciones configurables para el archivo vmware.log (continuación)

Parámetro	Descripción	Ejemplo	Notas
`log.fileLevel`	Controla el nivel mínimo en el que se escriben los mensajes en `vmware.log`. Cada mensaje de registro tiene un nivel asociado a él. Los niveles inferiores a la configuración especificada no se agregan a un archivo de registro de máquina virtual. Los niveles de registro de mensajes de la máquina virtual (desde el más restringido al menos restringido) son: ■ error ■ advertencia ■ notice ■ info (valor predeterminado) ■ registro detallado ■ depuración ■ depuración1 ■ depuración2 ■ depuración3 ■ depuración4 ■ depuración5 ■ depuración6 ■ depuración7 ■ depuración8 ■ depuración9 ■ depuración10	`log.fileLevel = "debug1"`	No establezca el nivel en un nivel más restrictivo que "info" para evitar que se filtren los mensajes necesarios para depurar los problemas de la máquina virtual. Baje el nivel por debajo de "info" solo cuando lo solicite el soporte con licencia. Restaure el ajuste a "info" una vez que finalice la depuración.
`log.filter.minLogLevel.<groupName>`	Controla la salida de los mensajes de depuración especializados.	`log.filter.minLogLevel.disklib = "debug5"`	Utilice esta opción solo cuando lo solicite el equipo de soporte con licencia, el cual debe proporcionar uno o varios parámetros `<groupName>`. Elimine el ajuste una vez que finalice la depuración.

Tabla 3-14. Opciones configurables para el archivo vmware.log (continuación)

Parámetro	Descripción	Ejemplo	Notas
`log.sysogID`	Permite el envío de mensajes de registro de máquina virtual al registrador del sistema de un host ESXi, como Syslog.	`log.syslogID = "vmx"`	Utilice "`vmx`" como valor para esta opción y permitir que el daemon de syslog de ESXi, `vmsyslogd`, envíe estos mensajes a un archivo de registro independiente.
`log.syslogLevel`	Controla el nivel mínimo en el cual se envían los mensajes al registrador del sistema de un host ESXi, como Syslog.	`log.syslogLevel = "debug"`	Los niveles y el funcionamiento de esta opción son idénticos a los de la opción `log.fileLevel`.

Cómo especificar la transmisión de mensajes a hosts remotos

Opcionalmente, puede configurar ESXi para que envíe mensajes de syslog a uno o varios hosts remotos, denominados recopiladores de syslog, como VMware vRealize Log Insight (anteriormente vCenter Log Insight), para recopilar mensajes de syslog.

Nota La práctica recomendada es configurar cada host ESXi para que envíe mensajes de syslog al menos a un recopilador de syslog. Esto ayuda a garantizar que los mensajes se conserven en caso de que se produzca un evento catastrófico del sistema y que pueda procesar mensajes de Syslog de diferentes maneras, como la categorización y el análisis en tiempo real (por ejemplo, por tipo, intervalo de tiempo o máquina), o archivar mensajes.

Utilice el ajuste de `Syslog.global.logHost` para definir las especificaciones del host remoto. Separe las especificaciones de varios hosts remotos con una coma (,). Después de configurar `Syslog.global.logHost`, los hosts ESXi abren y mantienen las conexiones con los recopiladores de syslog, y la transmisión de mensajes comienza inmediatamente. Cuando ESXi genera un mensaje de syslog, lo escribe en el archivo de registro adecuado en el host ESXi y también lo reenvía a todos los recopiladores de syslog configurados.

Además de los mensajes de syslog, también se pueden transmitir mensajes de auditoría a los recopiladores de syslog por motivos de seguridad. Los registros de auditoría realizan un seguimiento de la actividad relacionada con la seguridad en el host ESXi. Para obtener más información sobre los registros de auditoría, consulte Registros de auditoría.

Nota Consulte con el equipo de respuesta de seguridad de su empresa si hay que establecer registros de auditoría y cómo hacerlo. Por lo general, las configuraciones certificadas requieren que se habiliten los registros de auditoría.

Lo que sigue es la sintaxis para especificaciones de host remoto de `Syslog.global.logHost` :

```
protocol://target[:port]
```

Parámetro	Descripción	Notas
protocol	Especifica el protocolo de red. Los valores válidos son udp, tcp y ssl.	El protocolo ssl especifica que la transmisión de mensajes de syslog está cifrada. Los protocolos tcp y udp no cifran la transmisión. **Nota** Si la captura de mensajes de syslog o de auditoría es crucial para el sistema, evite utilizar el protocolo udp porque la infraestructura de redes externa a ESXi puede descartar mensajes UDP.
target	Especifica el host remoto. Puede utilizar una dirección IPV4 o IPv6 o un nombre de host.	Cuando utilice una dirección IPV6, debe insertarla entre corchetes [xxx], donde xxx es la dirección IPV6.
port	(Opcional) Especifica el puerto de host remoto que se utilizará. Si utiliza UDP o TCP. El puerto predeterminado es 1514. Si utiliza SSL. El puerto predeterminado es 514. Si decide utilizar puertos diferentes a 514 o 1514, debe ajustar el ESXi Firewall para abrir el puerto.	Para obtener más información sobre cómo abrir el firewall de ESXi para el puerto definido en cada especificación de host remoto, consulte Configurar el firewall de ESXi.

Ejemplos de especificaciones de máquina remota:

Ejemplo de cadena syslog.global.logHost	Notas
tcp://10.176.130.7:12345	Transmite mensajes de syslog a 10.176.130.7 mediante TCP/IP y el puerto 12345.
tcp://[2001:db8:85a3:8d3:1319:8a2e:370:7348]	Transmite mensajes de syslog a una dirección IPV6 mediante el puerto 1514.
tcp://[2001:db8:85a3:8d3:1319:8a2e:370:7348]:5432	Transmita mensajes de syslog a una dirección IPV6 mediante el puerto 54321.
udp://company.com	Transmite mensajes de syslog a company.com mediante UDP y el puerto 514.
udp://company.com,tcp://10.20.30.40:1050	Transmite mensajes de syslog a dos hosts remotos. El primer host remoto utiliza UDP para comunicarse con company.com mediante el puerto 514. El segundo host remoto utiliza TCP para comunicarse con la dirección IPV4 10.20.30.40 mediante el puerto 1050.
ssl://company.com	Transmite mensajes de syslog a company.com mediante SSL (TLS) y el puerto 514.

Longitud máxima de transmisión de mensajes

Si utiliza UDP, la longitud máxima de transmisión de mensajes de syslog es de 480 bytes para IPV4 y de 1180 bytes para IPV6.

Para TCP o SSL, la longitud máxima predeterminada de transmisión de mensajes de syslog es de 1 kibibyte (KiB). Puede aumentar esta longitud con el parámetro `Syslog.global.remoteHost.maxMsgLen`. El valor máximo es 16 KiB. Los mensajes de más de 16 KiB se truncan.

Nota Si es necesario aumentar la longitud máxima de transmisión, la práctica recomendada es aumentar la longitud solo lo específicamente necesario.

Aumentar la longitud máxima de los mensajes de syslog puede causar problemas si la infraestructura de redes y syslog externa a ESXi no puede controlar mensajes de más de 1 KiB.

Nota La práctica recomendada es no utilizar UDP para transmitir mensajes de syslog debido a las restricciones de longitud de paquetes y a la posibilidad de que la infraestructura de redes externas descarte los mensajes.

Consideraciones para los certificados al configurar transmisiones SSL a hosts remotos

Al configurar ESXi para transmitir mensajes de syslog a hosts remotos con SSL, debe agregar un certificado SSL para cada host remoto al almacén de CA de host ESXi. Para obtener más información, consulte Administrar certificados para hosts ESXi y Administrar certificados de CA con ESXCLI.

Nota Consulte la documentación de Syslog Collector sobre cómo configurar el recopilador para la recepción segura de mensajes de syslog mediante SSL y una clave privada.

Parámetros adicionales de transmisión de SSL

Un sistema ESXi que cumpla con los requisitos de certificación de seguridad puede requerir la habilitación de comprobaciones de X509 CRL. Para activar la configuración avanzada de `Syslog.global.certificate.strictX509Compliance` y `Syslog.global.certificate.checkCRL`, cambie el valor predeterminado de `false` a `true`. Debido a las limitaciones de implementación, si se habilitan las comprobaciones de CRL mediante la opción `Syslog.global.certificate.checkSSLCerts`, todos los certificados de una cadena de certificados deben proporcionar un vínculo de CRL. De forma predeterminada, la opción está habilitada. Puede desactivar las comprobaciones de certificados SSL si cambia el valor a `false`, pero esta no es una práctica recomendada. Es posible que deba desactivar las comprobaciones de certificados SSL al solucionar problemas de comunicación con un host remoto, pero solo durante un tiempo limitado.

Dónde encontrar la información del estado y el error del daemon de syslog

El daemon de syslog de ESXi utiliza el archivo de registro `/var/run/log/vmsyslogd.log` para almacenar información sobre el estado y los errores, incluidos los mensajes descartados. Si la transmisión de registros de auditoría está habilitada, el daemon de syslog también emite registros de auditoría relacionados con su funcionamiento, como las condiciones de inicio, detención y error del daemon, lo que le permite comprobar que el daemon de syslog se ejecute correctamente.

Cómo cambiar el área predeterminada de almacenamiento de archivos de registro de syslog

El área predeterminada de almacenamiento de archivos de registro de syslog es `/var/run/log`, local para cada host ESXi. Utilice la variable de configuración de syslog `Syslog.global.logDir` para cambiar el área predeterminada de almacenamiento de archivos de registro de syslog, siempre y cuando la ubicación resida en el almacenamiento persistente. Si `Syslog.global.logDir` se configura en un almacén persistente compartido por varios hosts ESXi para almacenar los archivos de registro de syslog, cambie el valor de `Syslog.global.logDirUnique` a `true` para que no se mezclen los registros. La opción `Syslog.global.logDirUnique` garantiza que cada máquina ESXi obtenga un nombre único que se agrega a la ruta `Syslog.global.logDir`, separando los archivos de registro de otros hosts.

Cola de mensajes de syslog para hosts remotos y descarte de mensajes

Una vez que se inician las emisiones de Syslog, nunca se detienen, excepto para reinicios y errores de ESXi, o una reconfiguración de Syslog para detenerse.

ESXi utiliza un mecanismo de cola al enviar mensajes de syslog a hosts remotos. Esto ayuda a evitar que se descarten mensajes si se encuentran y se resuelven problemas de conectividad de red. Sin embargo, si los problemas de conectividad duran más de lo que puede tolerar el mecanismo de cola, se descartan los mensajes de syslog. Puede ver las estadísticas sobre los descartes de mensajes en el archivo de registro del daemon de syslog.

Puede ver los mensajes descartados en /var/run/log/vmsyslogd-dropped.log. Este archivo de registro tiene ajustes de retención específicos, similares a los de los parámetros de retención específicos del programa. Los parámetros de retención de archivos de registro de mensajes descartados son: `Syslog.global.droppedMsgs.fileRotate` y `Syslog.global.droppedMsgs.fileSize`.

Configurar el filtrado de registros en hosts ESXi

Las capacidades de filtrado de registros permiten modificar la directiva de registro del servicio de Syslog que se ejecuta en un host ESXi.

A partir de vSphere 7.0 Update 2, puede agregar filtros de registro y habilitar el filtrado de registros mediante ESXCLI. Un filtro de registro, una vez establecido, permanece operativo hasta que se elimina, incluso después de reiniciar ESXi.

Los filtros de registro afectan a todos los eventos de registro que procesa el servicio de `vmsyslogd` del host ESXi, ya sea que se registren en un directorio de registro o en un servidor syslog remoto.

Debe habilitar la capacidad de filtrado de registros y volver a cargar el daemon de Syslog para activar los filtros de registros en el host ESXi.

Los comandos ESXCLI para configurar los filtros de registro siguen este patrón: `esxcli system syslog config logfilter {cmd} [cmd options]`.

Por ejemplo, para obtener la lista de filtros de registro disponibles, ejecute el siguiente comando: `[root@xxx-xx-dhcp-xx-xx:~] esxcli system syslog config logfilter list`.

Utilice el comando `set` para activar o desactivar el filtrado de registros: `[root@xxx-xx-dhcp-xx-xx:~] esxcli system syslog config logfilter set`.

Utilice el comando `add` para agregar un filtro de registro y el comando `remove` para eliminarlo.

Utilice el comando `get` para determinar si el filtrado de registros está habilitado.

Un filtro de registro se especifica mediante tres componentes y utiliza la siguiente sintaxis: `numLogs | ident | logRegexp`.

Parámetro	Descripción
`numLogs`	Especifica el número de coincidencias de la expresión regular de Python logRegexp que se permitirá antes de que comience el filtrado.
`ident`	La cadena `ident` es la forma en que una aplicación se identifica en la instalación de syslog. El filtro de `logRegexp` debe estar asociado a la misma aplicación. Para encontrar la cadena `ident` de una aplicación, inspeccione los archivos de registro en `/var/run/log`. El tercer campo de cada archivo de registro comienza con la cadena `ident` y termina con `[`.
`logRegexp`	Expresión regular de Python que identifica los mensajes que desea filtrar.

Por ejemplo, para filtrar todos los mensajes del daemon de hostd que contienen la palabra "mark" después de la décima aparición, utilice el siguiente comando: `esxcli system syslog config logfilter add --filter="10|Hostd|mark"`.

Para eliminar el filtro de registro, utilice el comando `esxcli system syslog config logfilter remove --filter="10|Hostd|mark"`.

Para obtener más información, consulte Opciones de syslog de ESXi.

Requisitos previos

Puede crear filtros de registros para reducir la cantidad de entradas repetidas en los registros de ESXi y agregar a la lista de no permitidos eventos de registros específicos en su totalidad.

Instale ESXCLI. Consulte *Introducción a ESXCLI*. Para solucionar problemas, ejecute los comandos de `esxcli` en ESXi Shell.

Usar vSphere Auto Deploy para reaprovisionar hosts

4

Puede reaprovisionar hosts ESXi implementados mediante vSphere Auto Deploy con un nuevo perfil de imagen para una versión diferente de ESXi.

Nota Si actualiza el host para que use una imagen de ESXi 6.0 o una versión posterior, el servidor vSphere Auto Deploy aprovisiona el host ESXi con certificados firmados por VMCA. Si actualmente está usando certificados personalizados, puede configurar el host para que use dichos certificados después de la actualización. Consulte *Seguridad de vSphere*.

Si se implementó un host usando vSphere Auto Deploy, es posible usar vSphere Auto Deploy para reaprovisionar el host con un nuevo perfil de imagen que contenga una versión diferente de ESXi. Puede usar vSphere ESXi Image Builder para crear y administrar perfiles de imagen. El servidor vSphere Auto Deploy se actualiza automáticamente si se actualiza el sistema vCenter Server correspondiente. A partir de la versión 6.0, el servidor vSphere Auto Deploy se encuentra siempre en el mismo nodo de administración que el sistema vCenter Server.

Lea los siguientes temas a continuación:

- Introducción a vSphere Auto Deploy
- Instalar y configurar vSphere Auto Deploy
- Reaprovisionar hosts

Introducción a vSphere Auto Deploy

vSphere Auto Deploy utiliza la infraestructura de arranque PXE con perfiles de host, una imagen deseada o una configuración en un nivel de clúster para aprovisionar hosts ESXi.

Información de estado de hosts ESXi

Nota No puede usar Auto Deploy en hosts ESXi configurados con DPU como parte de la función vSphere Distributed Services Engine.

Cuando se inicia un host físico configurado para vSphere Auto Deploy, vSphere Auto Deploy usa la infraestructura de arranque PXE junto con perfiles de host de vSphere, una imagen deseada o una configuración a nivel de clúster para aprovisionar y personalizar ese host. No se almacena ningún estado en el propio host. En su lugar, el servidor vSphere Auto Deploy administra la información de estado de cada host. vSphere Auto Deploy almacena la información de los hosts

ESXi que se van a aprovisionar en distintas ubicaciones. La información sobre la ubicación de los perfiles de imagen, los perfiles de host o los clústeres que administra mediante una sola imagen o mediante una configuración a nivel de clúster se especifica inicialmente en las reglas que asignan máquinas a perfiles de imagen y perfiles de host.

Tabla 4-1. vSphere Auto Deploy almacena información de implementación

Tipo de información	Descripción	Origen de información
Estado de imagen	El software ejecutable que se va a ejecutar en un host ESXi.	Perfil de imagen creado con vSphere ESXi Image Builder o una imagen de vSphere Lifecycle Manager.
Estado de configuración	Los parámetros que se pueden configurar, los cuales determinan el modo en que se configura el host; por ejemplo, conmutadores virtuales y su configuración, configuración de controladores y parámetros de arranque, etc.	Perfil de host creado mediante la interfaz de usuario del perfil de host o una configuración que se crea al configurar un clúster que administra todas las opciones del host ESXi a nivel de clúster en la interfaz de usuario de Inventory.
Estado dinámico	El estado de tiempo de ejecución que genera el software en ejecución; por ejemplo, claves privadas generadas o bases de datos de tiempo de ejecución.	Memoria de host, que se pierde durante el reinicio.
Estado de máquina virtual	Las máquinas virtuales almacenadas en un host y la información de inicio automático de máquinas virtuales (solo arranques posteriores).	La información de máquinas virtuales que envía vCenter Server a vSphere Auto Deploy debe estar disponible para suministrar información de máquinas virtuales a vSphere Auto Deploy.
Intervención del usuario	El estado basado en la intervención del usuario (por ejemplo, una dirección IP que el usuario proporciona cuando se inicia el sistema) no se puede incluir automáticamente en el perfil de host.	Información de personalización del host, almacenada por vCenter Server durante el primer arranque. Puede crear un perfil de host que requiera la intervención del usuario para determinados valores. Cuando vSphere Auto Deploy aplica un perfil de host para el que se requiere información que proporcionó el usuario, el host se coloca en modo de mantenimiento. Utilice la interfaz de usuario del perfil de host para comprobar el cumplimiento del perfil de host y responda al aviso para personalizar el host.

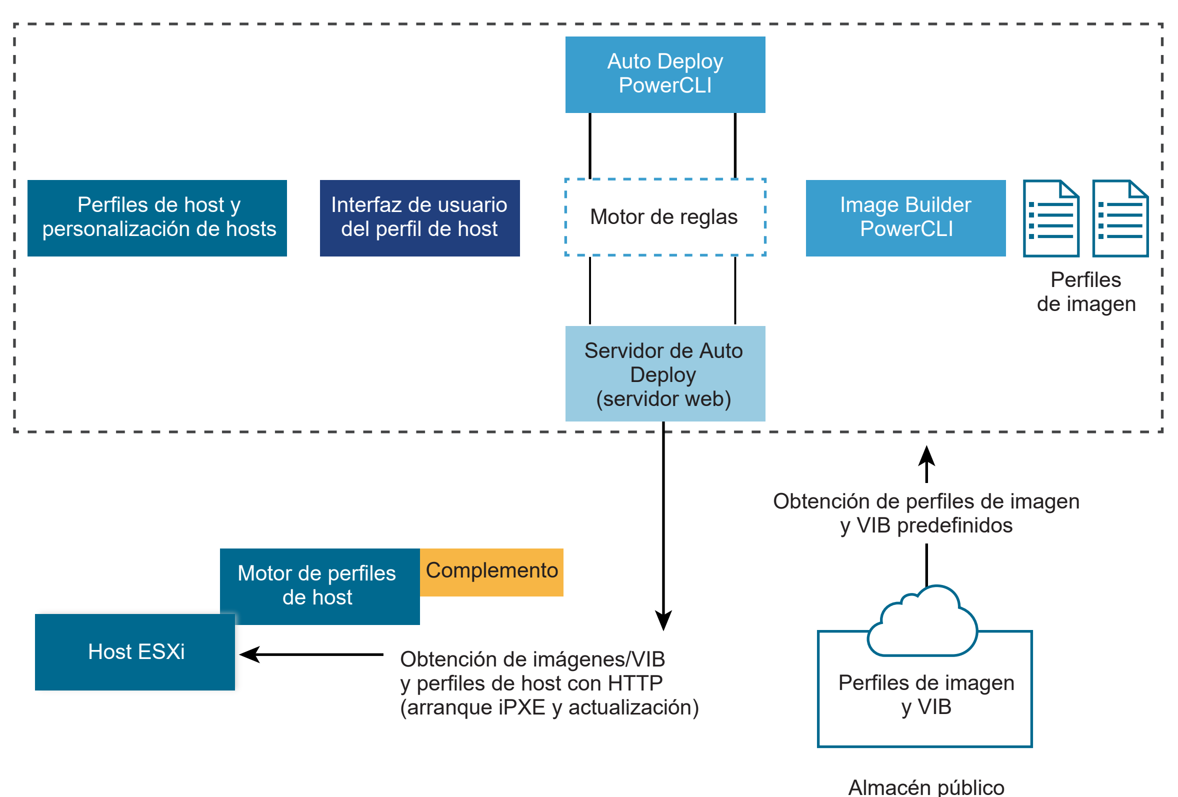
Arquitectura de vSphere Auto Deploy

La infraestructura de vSphere Auto Deploy consta de varios componentes.

Para obtener más información, vea el vídeo "Arquitectura de Auto Deploy":

 (Arquitectura de Auto Deploy)

Figura 4-1. Arquitectura de vSphere Auto Deploy



Servidor vSphere Auto Deploy

Sirve imágenes y perfiles de host a hosts ESXi.

Motor de reglas de vSphere Auto Deploy

Envía información al servidor vSphere Auto Deploy sobre qué perfil de imagen y qué perfil de host asignar a qué host. Los administradores utilizan vSphere Auto Deploy para definir las reglas que asignan perfiles de imagen y perfiles de host a los hosts.

Además de los perfiles de imagen heredados que se crean mediante los perfiles de host y VMware Image Builder, también se pueden crear reglas de vSphere Auto Deploy para implementar ESXi mediante una sola imagen de vSphere Lifecycle Manager o una configuración a nivel de clúster.

Perfiles de imagen

Defina el conjunto de VIB para arrancar hosts ESXi.

- VMware y los partners de VMware ponen perfiles de imagen y VIB a disposición en almacenes públicos. Utilice vSphere ESXi Image Builder para examinar el almacén y use el motor de reglas de vSphere Auto Deploy para especificar qué perfil de imagen se debe asignar a qué host.

- Se utilizan imágenes de vSphere Lifecycle Manager para aplicar actualizaciones de software y firmware a los hosts ESXi en un clúster. El uso de una sola imagen para administrar todos los hosts de un clúster garantiza la homogeneidad de la imagen del host en todo el clúster.
- Con ESXi 8.0, puede configurar un clúster que administre toda la configuración del host ESXi a nivel del clúster.
- Los clientes de VMware pueden crear un perfil de imagen personalizado basado en los perfiles de imagen y VIB públicos del almacén y aplicar ese perfil de imagen al host.

Perfiles de host

Defina la configuración específica de equipo, como parámetros de red o almacenamiento. Utilice la interfaz de usuario del perfil de host para crear perfiles de host. Puede crear un perfil de host para un host de referencia y aplicar dicho perfil a otros hosts del entorno para obtener una configuración coherente.

Nota Con ESXi 8.0, si configura un clúster que administre toda la configuración del host ESXi a nivel del clúster, no puede utilizar perfiles de host.

Personalizar hosts

Almacena información que el usuario proporciona cuando se aplican perfiles de host al host. La personalización de host podría contener direcciones IP u otra información que el usuario suministró para ese host. Para obtener más información sobre la personalización de host, consulte la documentación *Perfiles de host de vSphere*.

En las versiones anteriores de vSphere Auto Deploy, la personalización de host se denominaba archivo de respuesta.

Certificados de Auto Deploy

De manera predeterminada, el servidor Auto Deploy aprovisiona cada host con certificados firmados por VMware Certificate Authority (VMware CA). Para obtener más información, consulte Administrar certificados para hosts ESXi.

Como alternativa, si la directiva corporativa requiere que utilice certificados personalizados, puede configurar el servidor Auto Deploy para aprovisionar a todos los hosts con certificados personalizados que no estén firmados por VMware CA. El servidor Auto Deploy se transforma en una entidad de certificación subordinada a la entidad de certificación externa. En el modo de entidad de certificación personalizada, es responsable de administrar los certificados. No puede actualizar ni renovar certificados desde vSphere Client. En este modo, tampoco puede seleccionar solo un conjunto de hosts para aprovisionarlo con certificados personalizados, y puede firmar manualmente certificados personalizados solo para hosts con estado. Para obtener más información, consulte Usar certificados personalizados con Auto Deploy.

Con ESXi 8.0, Auto Deploy proporciona una tercera opción que le permite generar un certificado aparte de vSphere y pasar a ser independiente de la administración de certificados en vCenter Server. Por ejemplo, puede generar un certificado personalizado mediante un script personalizado o mediante un proveedor de servicios de registro de nombres de dominio, como Verisign. Puede utilizar certificados personalizados solo para un conjunto de hosts ESXi. También puede proporcionar certificados personalizados para hosts sin estado. Los hosts ESXi se identifican mediante la dirección MAC de la NIC que se utiliza para el arranque de red o el UUID del BIOS del host ESXi. VMware Endpoint Certificate Store (VECS) se actualiza con el certificado personalizado mediante PowerCLI. Para obtener más información sobre los nuevos cmdlets de PowerCLI, consulte Descripción general de cmdlets de vSphere Auto Deploy PowerCLI. VMware CA debe confiar en los certificados de ESXi personalizados, por lo que debe agregar el certificado público de CA para los certificados personalizados al almacén de TRUSTED_ROOTS en VECS. Auto Deploy también almacena los certificados personalizados y, cuando reconoce un host de arranque con la dirección MAC correspondiente de la NIC que se ha utilizado para el arranque de red o el UUID del BIOS del host ESXi, proporciona automáticamente el certificado personalizado. No es necesario que detenga o reinicie Auto Deploy ni vCenter Server cuando agregue un certificado personalizado a VECS; solo hay que reiniciar el host para el que cargue un certificado personalizado. Para obtener más información, consulte Usar certificados personalizados con Auto Deploy.

Instalar y configurar vSphere Auto Deploy

Antes de comenzar a usar vSphere Auto Deploy, debe preparar el entorno en varios pasos.

Comience con la configuración de los servidores y la preparación del hardware. Debe configurar el tipo de inicio para el servicio de vSphere Auto Deploy en el sistema vCenter Server que planea utilizar para administrar los hosts que aprovisione, y debe instalar vSphere PowerCLI.

Qué leer a continuación

- Lista de comprobación previa a la instalación de vSphere Auto Deploy

  Para poder iniciar las tareas en este escenario de vSphere Auto Deploy, primero debe asegurarse de que el entorno cumpla con los requisitos de hardware y software, y de contar con los permisos necesarios para los componentes que se incluyen en la configuración.

- Preparar el sistema para vSphere Auto Deploy

  Para poder realizar un arranque PXE de un host ESXi con vSphere Auto Deploy, primero es necesario instalar el software de los requisitos previos y configurar los servidores DHCP y TFTP con los que deberá interactuar vSphere Auto Deploy.

- Usar los cmdlets de vSphere Auto Deploy

  Los cmdlets de vSphere Auto Deploy se implementan como cmdlets de Microsoft PowerShell y se incluyen en vSphere PowerCLI. Los usuarios de los cmdlets de vSphere Auto Deploy pueden aprovechar todas las funciones de vSphere PowerCLI.

- Configurar licencias masivas

  Puede utilizar vSphere Client o ESXi Shell para especificar claves de licencia individuales o configurar licencias masivas mediante los cmdlets de vSphere PowerCLI. Las licencias masivas funcionan para todos los hosts ESXi, pero son especialmente útiles para los hosts aprovisionados con vSphere Auto Deploy.

Lista de comprobación previa a la instalación de vSphere Auto Deploy

Para poder iniciar las tareas en este escenario de vSphere Auto Deploy, primero debe asegurarse de que el entorno cumpla con los requisitos de hardware y software, y de contar con los permisos necesarios para los componentes que se incluyen en la configuración.

Tabla 4-2. Lista de verificación previa a la instalación

Software y hardware necesarios	Detalles
vCenter Server	El servidor vSphere Auto Deploy forma parte de vCenter Server. Debe habilitar e iniciar el servicio vSphere Auto Deploy en el sistema vCenter Server. Puede realizar muchas de las tareas de configuración iniciando sesión en vCenter Server. Consulte Preparar el sistema para vSphere Auto Deploy.
Almacenamiento	El almacenamiento para los almacenes de datos NFS, iSCSI o Fibre Channel de ESXi, con servidores y matrices de almacenamiento que se configuran de manera tal que los servidores puedan detectar los LUN. ■ Una lista de las direcciones IP de destino para NFS o iSCSI. ■ Una lista con la información de los volúmenes de destino para NFS o iSCSI.
Información del host (para cuatro hosts ESXi)	Una lista de las direcciones IP de destino para NFS o iSCSI. Una lista con la información de los volúmenes de destino para NFS o iSCSI. ■ La ruta predeterminada, la máscara de red y las direcciones IP de los servidores DNS principales y secundarios. ■ La dirección IP y la máscara de red de la red de administración principal de VMkernel. ■ La dirección IP y la máscara de red de las demás redes de VMkernel, como el almacenamiento, vSphere FT o VMware vMotion. vSphere Auto Deploy no sobrescribe las particiones existentes como opción predeterminada.
vSphere PowerCLI	Consulte Instalar PowerCLI.

Tabla 4-2. Lista de verificación previa a la instalación (continuación)

Software y hardware necesarios	Detalles
Almacén de software de ESXi	La ubicación del almacén de software de ESXi en la página de descargas del sitio web de VMware. Se debe usar una URL para apuntar al perfil de imagen que está almacenado en esa ubicación o se debe descargar un archivo .zip que funcione con un almacén local. No descargue la imagen de ESXi.
servidor TFTP	El software del instalador para TFTP, como un servidor TFTP de WinAgents.
Servidor DHCP	El servidor DHCP se incluye en las versiones de vSphere compatibles con Windows Server.
Servidor DNS	Un servidor DNS en funcionamiento. Es necesario agregar entradas tanto en Zona directa (Registro A) como en Zona inversa (Registro PTR) para cada host de destino.

También se necesita información acerca de los privilegios de administrador para los servidores principales del entorno, incluidos el servidor de Active Directory, el servidor DNS, el servidor DHCP, el servidor NTP, etc.

Se debe tener control completo del dominio de difusión de la subred en la que se implementa la configuración. Asegúrese de que no haya otros servidores DHCP, DNS ni TFTP en esta subred.

Preparar el sistema para vSphere Auto Deploy

Para poder realizar un arranque PXE de un host ESXi con vSphere Auto Deploy, primero es necesario instalar el software de los requisitos previos y configurar los servidores DHCP y TFTP con los que deberá interactuar vSphere Auto Deploy.

Si desea administrar vSphere Auto Deploy con cmdlets de PowerCLI, consulte *Configurar vSphere Auto Deploy y aprovisionar hosts con vSphere PowerCLI*.

Requisitos previos

- Compruebe que los hosts que desea aprovisionar con vSphere Auto Deploy cumplan los requisitos de hardware para ESXi. Consulte Requisitos de hardware de ESXi.
- Compruebe que los hosts ESXi tengan conectividad de red con vCenter Server y que se cumplan todos los requisitos de puerto. Consulte *Actualización de vCenter Server*.
- Compruebe que dispone de un servidor TFTP y un servidor DHCP en el entorno para enviar archivos y asignar direcciones de red a los hosts ESXi que aprovisiona Auto Deploy. Consulte #unique_86 y #unique_87.
- Compruebe que los hosts ESXi tengan conectividad de red a los servidores DHCP, TFTP y vSphere Auto Deploy.
- Si desea usar redes VLAN en el entorno de vSphere Auto Deploy, debe configurar las redes de extremo a extremo correctamente. Cuando el host realiza un arranque PXE, se debe configurar el controlador de firmware de manera que los marcos se etiqueten con los

identificadores de VLAN apropiados. Debe realizar los cambios apropiados en la interfaz UEFI/BIOS de forma manual para establecer esta configuración. De forma similar, debe configurar los grupos de puertos de ESXi correctamente con los identificadores de VLAN adecuados. Póngase en contacto con su administrador de red para obtener más información sobre la manera en la que los identificadores de VLAN se utilizan en el entorno.

- Asegúrese de contar con suficiente espacio de almacenamiento para el repositorio de vSphere Auto Deploy. El servidor vSphere Auto Deploy utiliza el repositorio para almacenar los datos que necesita, incluidos las reglas y los conjuntos de reglas que usted crea, así como los VIB y los perfiles de imagen que se especifican en las reglas.

  Se recomienda asignar 2 GB para que haya suficiente espacio para almacenar cuatro perfiles de imagen y quede espacio adicional. Cada perfil de imagen requiere aproximadamente 400 MB. Determine la cantidad de perfiles de imagen que espera utilizar para definir la cantidad de espacio que debe reservar para el repositorio de vSphere Auto Deploy.

- Otorgue privilegios administrativos al servidor DHCP que administra el segmento de red desde el cual desea realizar el arranque. Puede utilizar un servidor DHCP que ya se encuentre en el entorno, o bien instalarlo. Para la configuración de vSphere Auto Deploy, reemplace el nombre de archivo `gpxelinux.0` con `snponly64.efi.vmw-hardwired` para UEFI o `undionly.kpxe.vmw-hardwired` para BIOS. Para obtener más información sobre las configuraciones de DHCP, consulte Configuraciones de DHCP de muestra.

- Proteja la red como lo haría para cualquier otro método de implementación basado en PXE. vSphere Auto Deploy transfiere datos por SSL para evitar interferencias accidentales e intromisiones. No obstante, la autenticidad del cliente o del servidor vSphere Auto Deploy no se comprueba durante el arranque PXE.

- Si desea administrar vSphere Auto Deploy con cmdlets de PowerCLI, compruebe que Microsoft .NET Framework 4.5 o 4.5.x y Windows PowerShell 3.0 o 4.0 se encuentren instalados en un equipo Windows. Consulte *Guía del usuario de vSphere PowerCLI*.

- Configure un servidor remoto de Syslog. Consulte la documentación de *Administrar vCenter Server y hosts* para obtener información sobre la configuración del servidor de Syslog. Configure el primer host que arranque para que use el servidor remoto de Syslog y aplique el perfil de host de dicho host a todos los demás hosts de destino. De forma opcional, instale y utilice VMware vCenter Log Insight, que proporciona agregación y análisis de registros para productos VMware y productos que no son VMware, virtuales y físicos, con búsqueda y análisis de eventos de registro casi en tiempo real.

- Instale ESXi Dump Collector, configure el primer host de manera que todos los volcados de memoria del núcleo se direccionen a ESXi Dump Collector y aplique el perfil de host de ese host a todos los otros hosts.

- Si los hosts que planea aprovisionar con vSphere Auto Deploy presentan un BIOS heredado, compruebe que el servidor vSphere Auto Deploy tenga una dirección IPv4. El arranque PXE con firmware de BIOS heredado solo se puede realizar mediante IPv4. El arranque PXE con firmware UEFI se puede realizar mediante IPv4 o IPv6.

Procedimiento

1 Desplácese hasta **Inicio > Auto Deploy**.

   De forma predeterminada, solo la función de administrador tiene privilegios para usar el servicio vSphere Auto Deploy.

2 En la página **Auto Deploy**, seleccione la instancia de vCenter Server en el menú desplegable en la parte superior.

3 Haga clic en **Habilitar Auto Deploy e Image Builder** para activar el servicio.

   Si el servicio de **Image Builder** ya está activo, seleccione la pestaña **Configurar** y haga clic en **Habilitar servicio de Auto Deploy**.

   Aparecerá la página **Almacén de software**.

4 Configure el servidor TFTP.

   a Haga clic en la pestaña **Configurar**.

   b Haga clic en **Descargar ZIP de arranque TFTP** para descargar el archivo de configuración de TFTP y, a continuación, descomprima el archivo en el directorio en el que el servidor TFTP almacena los archivos.

   c (opcional) Para utilizar un servidor proxy, haga clic en **Agregar** en el panel *Resumen de tiempo de ejecución de Auto Deploy* e introduzca una dirección URL del servidor proxy en el cuadro de texto.

      Mediante el proxy inverso, los servidores pueden descargar las solicitudes realizadas al servidor vSphere Auto Deploy.

5 Configure el servidor DHCP de manera que apunte al servidor TFTP en el que se encuentra el archivo ZIP de TFTP.

   a Especifique la dirección IP del servidor TFTP en la opción 66 del DHCP, la cual se suele llamar next-server.

   b Especifique el nombre de archivo de arranque, que es `snponly64.efi.vmw-hardwired` para UEFI o `undionly.kpxe.vmw-hardwired` para BIOS, en la opción 67 de DHCP, a menudo denominado `boot-filename`.

6 Configure todos los hosts que desea aprovisionar con vSphere Auto Deploy para realizar un arranque de red o un arranque PXE, según las instrucciones del fabricante.

7 (opcional) Si configura el entorno de manera que se utilice el modo de huellas digitales, puede reemplazar el certificado `rbd-ca.crt` de OpenSSL y la clave privada `rbd-ca.key` de OpenSSL por un certificado y una clave privada personales para utilizar su propia entidad de certificación (Certificate Authority, CA).

   Los archivos se encuentran en `/etc/vmware-rbd/ssl/`.

   De forma predeterminada, vCenter Server usa VMware Certificate Authority (VMCA).

Resultados

Cuando inicia un host ESXi que está configurado para vSphere Auto Deploy, el host se comunica con el servidor DHCP y se redirige al servidor vSphere Auto Deploy, el cual aprovisiona el host con el perfil de imagen especificado en el conjunto de reglas activas.

Pasos siguientes

- Puede cambiar las propiedades de configuración predeterminadas del **Servicio Auto Deploy**. Para obtener más información, consulte "Configurar vCenter Server" en la documentación de *Administrar vCenter Server y hosts*.
- Puede cambiar las propiedades de configuración predeterminadas del **Servicio Image Builder**. Para obtener más información, consulte "Configurar vCenter Server" en la documentación de *Administrar vCenter Server y hosts*.
- Defina una regla que asigne un perfil de imagen y un perfil de host opcional, ubicación de host o paquete de scripts al host.
- (opcional) Configure el primer host que aprovisione como un host de referencia. Utilice el almacenamiento y la red, entre otras opciones que desea que el host de destino comparta. Cree un perfil de host para el host de referencia y escriba una regla que asigne tanto el perfil de imagen que ya se ha probado como el perfil de host a los hosts de destino.
- (opcional) Si desea que vSphere Auto Deploy sobrescriba las particiones existentes, configure un host de referencia de manera que realice la partición de forma automática y, a continuación, aplique el perfil de host del host de referencia a otros hosts.
- (opcional) Si debe configurar información específica de un host, configure el perfil de host del host de referencia de manera que solicite la interacción del usuario. Para obtener más información sobre la personalización de host, consulte la documentación *Perfiles de host de vSphere*.

Usar los cmdlets de vSphere Auto Deploy

Los cmdlets de vSphere Auto Deploy se implementan como cmdlets de Microsoft PowerShell y se incluyen en vSphere PowerCLI. Los usuarios de los cmdlets de vSphere Auto Deploy pueden aprovechar todas las funciones de vSphere PowerCLI.

Los usuarios experimentados de PowerShell también pueden utilizar los cmdlets de vSphere Auto Deploy del mismo modo que los cmdlets de PowerShell. Si no está familiarizado con PowerShell y vSphere PowerCLI, las sugerencias siguientes pueden ser de utilidad.

Puede escribir cmdlets, parámetros y valores de parámetros en el shell de vSphere PowerCLI.

- Obtenga ayuda para cualquier cmdlet a través de `Get-Help`*`cmdlet_name`*.
- Recuerde que PowerShell no distingue mayúsculas de minúsculas.
- Utilice la opción de finalización con tabulación para los nombres de cmdlets y parámetros.

- Puede aplicar formato a cualquier resultado de cmdlet o variable mediante `Format-List` o `Format-Table`, o mediante sus formas abreviadas: `fl` o `ft`. Para obtener más información, ejecute el cmdlet `Get-Help Format-List`.

Transmitir parámetros por nombre

Puede transmitir parámetros por nombre en la mayoría de los casos y rodear los valores de parámetros que contienen espacios o caracteres especiales con comillas dobles.

```
Copy-DeployRule -DeployRule testrule -ReplaceItem MyNewProfile
```

La mayoría de los ejemplos de la documentación *Instalar y configurar vCenter Server* transmiten parámetros por nombre.

Transmitir parámetros como objetos

Puede transmitir parámetros como objetos si desea ejecutar scripts y automatización. Transmitir parámetros como objetos resulta útil con los cmdlets que devuelven varios objetos y con los cmdlets que devuelven un solo objeto. Tenga en cuenta el ejemplo siguiente:

1 Vincule a una variable el objeto que contiene la información de cumplimiento de normas de un conjunto de reglas para un host.

   ```
   $tr = Test-DeployRuleSetCompliance MyEsxi42
   ```

2 Vea la propiedad `itemlist` del objeto para determinar la diferencia entre lo que contiene el conjunto de reglas y lo que usa el host actualmente.

   ```
   $tr.itemlist
   ```

3 Corrija el host para que use el conjunto de reglas modificado, utilizando el cmdlet `Repair-DeployRuleSetCompliance` con la variable.

   ```
   Repair-DeployRuleSetCompliance $tr
   ```

En este ejemplo, se corrige el host la próxima vez que se arranca.

Configurar licencias masivas

Puede utilizar vSphere Client o ESXi Shell para especificar claves de licencia individuales o configurar licencias masivas mediante los cmdlets de vSphere PowerCLI. Las licencias masivas funcionan para todos los hosts ESXi, pero son especialmente útiles para los hosts aprovisionados con vSphere Auto Deploy.

La asignación de claves de licencia mediante vSphere Client y la asignación de licencias mediante los cmdlets de vSphere PowerCLI funcionan de manera diferente.

Asignación de claves de licencia mediante vSphere Client

Puede asignar claves de licencia a un host al agregar el host al sistema vCenter Server o cuando un sistema vCenter Server administra el host.

Asignar claves de licencia mediante LicenseDataManager vSphere PowerCLI

Puede especificar un conjunto de claves de licencia para agregar a un conjunto de hosts. Las claves de licencia se agregan a la base de datos de vCenter Server. Cada vez que se agrega un host al sistema vCenter Server o vuelve a conectarse a él, se le asigna una clave de licencia. Una clave de licencia que se asigna mediante vSphere PowerCLI se trata como una clave de licencia predeterminada. Cuando se agrega o se vuelve a conectar un host sin licencia, se le asigna la clave de licencia predeterminada. Si un host ya tiene licencia, mantiene su clave de licencia.

En el ejemplo siguiente, se asignan licencias a todos los hosts de un centro de datos. También puede asociar licencias con hosts y clústeres.

El ejemplo siguiente está destinado a usuarios avanzados de vSphere PowerCLI que saben cómo usar variables de PowerShell.

Requisitos previos

Preparar el sistema para vSphere Auto Deploy.

Procedimiento

1 En una sesión de vSphere PowerCLI, conéctese al sistema vCenter Server que desea utilizar y vincule el administrador de licencias asociado a una variable.

```
Connect-VIServer -Server 192.XXX.X.XX -User username -Password password
$licenseDataManager = Get-LicenseDataManager
```

2 Ejecute un cmdlet que recupere el centro de datos donde se encuentran los hosts para los cuales desea utilizar la función de licencias masivas.

```
$hostContainer = Get-Datacenter -Name Datacenter-X
```

También puede ejecutar un cmdlet que recupere un clúster con la finalidad de utilizar licencias masivas para todos los hosts de un clúster, o que recupere una carpeta con la finalidad de utilizar licencias masivas para todos los hosts de una carpeta.

3 Cree un objeto `LicenseData` y un objeto `LicenseKeyEntry` con la clave de licencia y el identificador de tipo asociados.

```
$licenseData = New-Object VMware.VimAutomation.License.Types.LicenseData
$licenseKeyEntry = New-Object Vmware.VimAutomation.License.Types.LicenseKeyEntry
$licenseKeyEntry.TypeId = "vmware-vsphere"
$licenseKeyEntry.LicenseKey = "XXXXX-XXXXX-XXXXX-XXXXX-XXXXX"
```

4 Asocie el atributo `LicenseKeys` del objeto `LicenseData` que creó en el paso 3 con el objeto `LicenseKeyEntry`.

```
$licenseData.LicenseKeys += $licenseKeyEntry
```

5 Actualice los datos de licencias del centro de datos con el objeto `LicenseData` y compruebe que la licencia esté asociada con el contenedor de host.

```
$licenseDataManager.UpdateAssociatedLicenseData($hostContainer.Uid, $licenseData)
$licenseDataManager.QueryAssociatedLicenseData($hostContainer.Uid)
```

6 Aprovisione un host o más con vSphere Auto Deploy y asígnelos al centro de datos o al clúster al que asignó los datos de licencias.

7 Puede usar vSphere Client para verificar que el host se haya asignado correctamente a la licencia predeterminada `XXXXX-XXXXX-XXXXX-XXXXX-XXXXX`.

Resultados

Todos los hosts que se hayan asignado al centro de datos ahora cuentan con licencia de manera automática.

Reaprovisionar hosts

Utilice vSphere Auto Deploy para reaprovisionar hosts ESXi con un perfil de imagen o un perfil de host diferente.

vSphere Auto Deploy admite varias opciones de reaprovisionamiento. Puede realizar un reinicio o un reaprovisionamiento sencillos con otro perfil de imagen o de host.

Para un primer arranque con vSphere Auto Deploy, debe configurar el entorno y agregar reglas al conjunto de reglas. Consulte el tema “Prepararse para vSphere Auto Deploy” en la documentación sobre *instalación y configuración de vSphere*.

Están disponibles las siguientes operaciones de reaprovisionamiento.

- Reinicio simple.
- Reinicio de hosts sobre los que el usuario respondió preguntas durante la operación de arranque.
- Reaprovisionamiento con un perfil de imagen diferente.
- Reaprovisionamiento con un perfil de host diferente.

Reaprovisionar hosts con operaciones de reinicio simples

Puede reaprovisionar hosts ESXi con el perfil de imagen, el perfil de host, el script personalizado y la ubicación de vCenter Server asignada durante el primer arranque.

Requisitos previos

El reinicio simple de un host aprovisionado con vSphere Auto Deploy solo requiere que se sigan cumpliendo todos los requisitos previos. El proceso utiliza el perfil de imagen asignado previamente, el perfil de host, el script personalizado y la ubicación de vCenter Server.

- Compruebe que la configuración que realizó durante la primera operación de arranque esté vigente.
- Compruebe que todos los elementos asociados se encuentren disponibles. Un elemento puede ser un perfil de imagen, un perfil de host, un script personalizado o una ubicación de inventario de vCenter Server.
- Compruebe que el host contenga la información de identificación (etiqueta de activo, dirección IP) que tenía en las operaciones de arranque anteriores.

Procedimiento

1 Coloque el host en modo de mantenimiento.

Tipo de host	Acción
El host es parte de un clúster de DRS	VMware DRS migra las máquinas virtuales a los hosts adecuados cuando coloca el host en modo de mantenimiento.
El host no es parte de un clúster de DRS	Debe migrar todas las máquinas virtuales a distintos hosts y poner todos los hosts en modo de mantenimiento.

2 Reinicie el host.

Resultados

El host se apaga. Al reiniciarse, el host utiliza el perfil de imagen que proporciona el servidor vSphere Auto Deploy. El servidor vSphere Auto Deploy también aplica el perfil de host almacenado en el sistema vCenter Server.

Usar vSphere PowerCLI para reaprovisionar un host

Puede utilizar vSphere Auto Deploy para reaprovisionar un host con un nuevo perfil de imagen en una sesión de vSphere PowerCLI.

Existen varias opciones para reaprovisionar hosts.

- Si los VIB que desea usar son compatibles con la actualización directa, puede usar un comando `esxcli software vib update`. En ese caso, también debe actualizar el conjunto de reglas que se va a usar en un perfil de imagen que incluya los nuevos VIB.
- Durante las pruebas, puede aplicar un perfil de imagen a un host individual con el cmdlet `Apply-EsxImageProfile` y reiniciar el host para que el cambio sea efectivo. El cmdlet `Apply-EsxImageProfile` actualiza la asociación entre el host y el perfil de imagen, pero no instala ningún VIB en el host.
- En todos los demás casos, utilice este procedimiento.

Requisitos previos

- Compruebe que el perfil de imagen que desea utilizar para reaprovisionar el host se encuentre disponible. Utilice vSphere ESXi Image Builder en una sesión de vSphere PowerCLI. Consulte "Usar vSphere ESXi Image Builder CLI" en la documentación sobre *instalación y configuración de vSphere*.
- Compruebe que la configuración que realizó durante la primera operación de arranque esté vigente.

Procedimiento

1 En la indicación de PowerShell, ejecute el cmdlet `Connect-VIServer` vSphere PowerCLI para conectarse al sistema vCenter Server con el que se registró vSphere Auto Deploy.

```
Connect-VIServer ipv4_or_ipv6_address
```

Es posible que el cmdlet devuelva una advertencia de certificado de servidor. En un entorno de producción, asegúrese de que no se emita ninguna advertencia de certificado de servidor. En un entorno de desarrollo, puede omitir la advertencia.

2 Determine la ubicación de un almacén de software público que contenga el perfil de imagen que desea utilizar o defina un perfil de imagen personalizado con vSphere ESXi Image Builder.

3 Ejecute `Add-EsxSoftwareDepot` para agregar el almacén de software que contiene el perfil de imagen a la sesión de vSphere PowerCLI.

Tipo de almacén	Cmdlet
Almacén remoto	Ejecute **`Add-EsxSoftwareDepot`** ***`url_del_almacén`***.
Archivo ZIP	a Descargue el archivo ZIP en una ruta de acceso de archivos local o cree un punto de montaje local en el equipo de vSphere PowerCLI. b Ejecute **`Add-EsxSoftwareDepot C:\file_path\my_offline_depot.zip`**.

4 Ejecute `Get-EsxImageProfile` para ver una lista de perfiles de imagen y determine qué perfil desea utilizar.

5 Ejecute `Copy-DeployRule` y especifique el parámetro `ReplaceItem` para cambiar la regla que asigna un perfil de imagen a hosts.

El siguiente cmdlet reemplaza el perfil de imagen actual que la regla asigna al host con el perfil *my_new_imageprofile*. Cuando el cmdlet finaliza, `myrule` asigna el nuevo perfil de imagen a los hosts. Se cambia el nombre de la antigua versión de `myrule` y se la oculta.

```
Copy-DeployRule myrule -ReplaceItem my_new_imageprofile
```

6 Pruebe el cumplimiento de reglas para cada host en el que desee implementar la imagen.

   a Compruebe que pueda acceder al host para el cual desea probar el cumplimiento del conjunto de reglas.

```
Get-VMHost -Name ESXi_hostname
```

   b Ejecute el cmdlet que prueba el cumplimiento del conjunto de reglas para el host y vincule el valor devuelto a una variable para usarlo en otro momento.

```
$tr = Test-DeployRuleSetCompliance ESXi_hostname
```

   c Examine las diferencias entre el contenido del conjunto de reglas y la configuración del host.

```
$tr.itemlist
```

   El sistema devolverá una tabla de elementos actuales y esperados si el host en el que se desea probar el cumplimiento de un nuevo conjunto de reglas cumple con el conjunto de reglas activo.

```

CurrentItem                            ExpectedItem
-----------                            ------------
my_old_imageprofile                          my_new_imageprofile
```

   d Corrija el host para que use el conjunto de reglas modificado la próxima vez que arranque.

```
Repair-DeployRuleSetCompliance $tr
```

7 Reinicie el host para aprovisionarlo con el nuevo perfil de imagen.

Escribir una regla y asignar un perfil de host a hosts

vSphere Auto Deploy puede asignar un perfil de host a uno o más hosts ESXi.

En muchos casos, puede asignar un host a un clúster en lugar de especificar un perfil de host explícitamente. El host utiliza el perfil de host del clúster.

Requisitos previos

El perfil de host puede incluir información sobre la configuración de almacenamiento, la configuración de red u otras características del host. Si agrega un host a un clúster, se utiliza el perfil de host de ese clúster.

- Instale PowerCLI y todo el software de requisito previo. Para obtener información, consulte Instalar y configurar vCenter Server.
- Exporte el perfil de host que desea utilizar.

Procedimiento

1 En una sesión de PowerCLI, ejecute el cmdlet `Connect-VIServer` para conectarse al sistema vCenter Server con el que se registró vSphere Auto Deploy.

```
Connect-VIServer ipv4_or_ipv6_address
```

Es posible que el cmdlet devuelva una advertencia de certificado de servidor. En un entorno de producción, asegúrese de que no se emita ninguna advertencia de certificado de servidor. En un entorno de desarrollo, puede omitir la advertencia.

2 Con vSphere Client, configure un host con los parámetros que desee usar y cree un perfil de host a partir de él.

3 Busque el nombre del perfil de host mediante la ejecución del cmdlet `Get-VMhostProfile` de PowerCLI, pasando el host ESXi a partir del cual creó un perfil de host.

4 En el símbolo de PowerCLI, defina una regla en la que los perfiles de host se asignen a hosts con ciertos atributos; por ejemplo, un intervalo de direcciones IP.

```
New-DeployRule -Name "testrule2" -Item my_host_profile -Pattern "vendor=Acme,Zven",
"ipv4=192.XXX.1.10-192.XXX.1.20"
```

El elemento especificado se asigna a todos los hosts que posean los atributos especificados. Este ejemplo especifica una regla denominada testrule2. Esta asigna el perfil de host especificado *mi_perfil_de_host* a todos los hosts que tengan una dirección IP dentro del intervalo especificado y cuyo fabricante sea Acme o Zven.

5 Agregue la regla al conjunto de reglas.

```
Add-DeployRule testrule2
```

De forma predeterminada, el conjunto de reglas en funcionamiento se convierte en el conjunto de reglas activo y los cambios en él se vuelven activos cuando agrega una regla. Si utiliza el parámetro `NoActivate`, el conjunto de reglas en funcionamiento no se convierte en el conjunto de reglas activo.

Pasos siguientes

- Asigne un host ya aprovisionado con vSphere Auto Deploy al nuevo perfil de host. Para ello, realice operaciones de prueba de cumplimiento y reparación en esos hosts. Para obtener más información, consulte Probar y reparar cumplimiento de reglas .
- Encienda los hosts no aprovisionados para aprovisionarlos con el perfil de host.

Probar y reparar cumplimiento de reglas

Pruebe el cumplimiento de las reglas nuevas o modificadas y repare según corresponda, ya que los cambios en el conjunto de reglas de vSphere Auto Deploy no se actualizan automáticamente.

Requisitos previos

Cuando se agrega una regla al conjunto de reglas de vSphere Auto Deploy o cuando se modifican una o más reglas, los hosts no se actualizan de manera automática. vSphere Auto Deploy aplica las reglas nuevas únicamente cuando se prueba el cumplimiento de reglas y se realizan las correcciones pertinentes.

- Prepare el sistema e instale el servidor Auto Deploy. Para obtener más información, consulte Preparar el sistema para vSphere Auto Deploy.
- Compruebe que la infraestructura incluya un host ESXi o más aprovisionados con vSphere Auto Deploy y que el host en el que se instaló PowerCLI pueda acceder a esos hosts ESXi.

Procedimiento

1 En una sesión de PowerCLI, ejecute el cmdlet `Connect-VIServer` para conectarse al sistema vCenter Server con el que se registró vSphere Auto Deploy.

```
Connect-VIServer ipv4_or_ipv6_address
```

Es posible que el cmdlet devuelva una advertencia de certificado de servidor. En un entorno de producción, asegúrese de que no se emita ninguna advertencia de certificado de servidor. En un entorno de desarrollo, puede omitir la advertencia.

2 Use PowerCLI para comprobar qué reglas de vSphere Auto Deploy están disponibles actualmente.

```
Get-DeployRule
```

El sistema devuelve las reglas y los patrones, y los elementos asociados.

3 Modifique una de las reglas disponibles.

Por ejemplo, puede cambiar el perfil de imagen y el nombre de la regla.

```
Copy-DeployRule -DeployRule testrule -ReplaceItem MyNewProfile
```

No se puede editar una regla que ya se agregó a un conjunto de reglas activo. En lugar de ello, puede copiar la regla y reemplazar el elemento o el patrón que desea cambiar.

4 Compruebe que pueda acceder al host para el cual desea probar el cumplimiento del conjunto de reglas.

```
Get-VMHost -Name MyEsxi42
```

5 Ejecute el cmdlet que prueba el cumplimiento del conjunto de reglas para el host y vincule el valor devuelto a una variable para usarlo en otro momento.

```
$tr = Test-DeployRuleSetCompliance MyEsxi42
```

6 Examine las diferencias entre el contenido del conjunto de reglas y la configuración del host.

```
$tr.itemlist
```

Si el host para el que desea probar el cumplimiento del nuevo conjunto de reglas cumple con el conjunto de reglas activo, el sistema devuelve una tabla de elementos actuales y esperados.

```
CurrentItem                             ExpectedItem
-----------                             ------------
My Profile 25                           MyNewProfile
```

7 Corrija el host para que use el conjunto de reglas modificado la próxima vez que arranque.

```
Repair-DeployRuleSetCompliance $tr
```

Pasos siguientes

Si la regla que modificó ha especificado la ubicación en el inventario, el cambio se aplica cuando se corrigen los problemas de cumplimiento. Para todos los demás cambios, reinicie el host para que vSphere Auto Deploy aplique la nueva regla y logre el cumplimiento entre el conjunto de reglas y el host.

Recopilar registros para solución de problemas de hosts ESXi

5

Puede recopilar archivos de registro de instalación o actualización para ESXi que le ayuden a identificar el origen del error si se produce un error en una instalación o actualización.

Solución

1 Introduzca el comando `vm-support` en ESXi Shell o mediante SSH.

2 Desplácese hasta el directorio `/var/tmp/`.

3 Recupere los archivos de registro desde el archivo `.tgz`.